ADVANCED ALGEBRA

VOLUME III

G. Bell and Sons Ltd
Portugal Street, London

Calcutta, Bombay & Madras
Longmans, Green & Co. Ltd

Toronto
Clarke, Irwin & Co. Ltd

ADVANCED ALGEBRA

VOLUME III

BY

CLEMENT V. DURELL, M.A.

AUTHOR OF "GENERAL ARITHMETIC", "A NEW ALGEBRA FOR SCHOOLS", ETC.
JOINT AUTHOR OF "ADVANCED TRIGONOMETRY", "ELEMENTARY CALCULUS", ETC.

AND

A. ROBSON, M.A.

SENIOR MATHEMATICAL MASTER, MARLBOROUGH COLLEGE
JOINT AUTHOR OF "ADVANCED TRIGONOMETRY", "ELEMENTARY CALCULUS", ETC

LONDON
G. BELL AND SONS, LTD

1946

First published 1937.
Reprinted 1943, 1945, 1946.

PRINTED IN GREAT BRITAIN BY ROBERT MACLEHOSE AND CO. LTD.
THE UNIVERSITY PRESS, GLASGOW

PREFACE

VOLUMES II and III complete the school course including suitable work for university scholars in their last terms at school.

The authors have attempted to concentrate attention on the fundamental principles, methods and notation which furnish the tools necessary for more advanced work. They believe that many of the topics which constitute the conventional course are only of value in so far as they illustrate general ideas, and that much of what has been called 'higher algebra' in the school course should be scrapped. Only the requirements of certain examinations have prevented them from pursuing a more drastic policy than they have actually adopted.

The account of the difference (Δ) notation in Chapter X forms an introduction to the study of difference equations in Chapter XI, and taken in conjunction with the sketch of the principles of probability in Chapter XVIII should enable those concerned with actuarial work to learn the essentials of these subjects before taking a specialist course. Some of the examples on probability may appear to be remote from actual life, but the more practical applications do not always provide the simplest illustrations of the principles involved. The philosophy of probability lies outside the scope of this work.

Difference equations, or recurrence formulae, are of great importance in mathematics, even apart from their valuable analogy with differential equations. Recurring series and continued fractions at least have the merit of providing illustrations of difference methods.

In Chapter XII the distinction between theorems of real and complex algebra is emphasised and for this purpose the authors believe that the new terminology introduced on p. 253 will be

found of real service to the student: the mature mathematician may find it unnecessary. The main theme of this chapter is the fundamental theorem about $Af+Bg=1$, and special care has been taken to show how the theory of partial fractions can be derived from it. In practical decomposition into partial fractions the choice of the best method is a matter of experience and therefore the various alternatives have been copiously illustrated by examples in the text.

In Chapter XIII Descartes' Rule of Signs has been treated more fully than usual and its special value with incomplete equations has been emphasised. The importance of the considerations of weight and order in the theory of symmetric functions of the roots of an equation has been stressed. Newton's formula has been enunciated in a form slightly more comprehensive than is customary.

The early part of Chapter XIV is of great importance, because a sound understanding of the principles of convergence is essential; but the developments in the later part of the chapter should be left for a second reading. Although inequalities are not discussed systematically until Chapter XV, simple examples of their manipulation necessarily occur in Chapter XIV and the fundamental logarithmic inequality which was given on p. 108 of Volume I is required in some of the examples.

In Chapters XV, XVI, XVII the student is introduced to subjects of special significance in modern mathematics. Although he may be well-advised to rely at first on *ab initio* methods in dealing with inequalities, he can profitably make a start at learning the forms into which the simple special results can be generalised. To pursue this subject further he will naturally take up the study of *Inequalities* by Hardy, Littlewood, and Pólya. Attention is called to the introduction of the δ- and ϵ- symbols and the use of dummy suffixes. Too often the young student at the university is plunged into some subject in which these are the normal working tools, although he has had no preliminary training in their use. The same applies with even greater force to matrices.

The subject of Chapter XIX is a fascinating one. Any pure mathematician is certain to be attracted by it, even though the account here given does not give much indication of the lines of modern research in Theory of Numbers.

For the convenience of teachers, the exercises are divided into sections **A**, **B**, **C**: both the **A** and **B** questions are straightforward applications of the bookwork. It is suggested that all the **A** questions should be done. The **B** questions are intended for extra practice when this is necessary. The **C** questions are harder but have been carefully graded.

Short books of **Hints** for the solutions of any examples that are not immediate deductions from the bookwork have been compiled for Volumes II and III and it is suggested that the student should have access to these books. Teachers cannot always find time to discuss various methods of handling a problem, and, even when the student has not failed to discover a solution, it will often be helpful to him to compare his method with another. The hints consist, in effect, of a very large number of illustrative examples solved in outline.

An index to Volumes I, II, III is given at the end of Volume III.

The thanks of the authors are due to Mr. W. Hope-Jones of Eton and Mr. T. A. A. Broadbent for advice on the probability and sequence chapters respectively, and to Mr. P. Hall of King's College and Mr. W. G. Welchman of Sidney Sussex College for advice about matrices. They have again to thank Mr. J. C. Manisty for valuable assistance at the proof stage.

A. R.

June, 1937 C. V. D.

CONTENTS

VOLUME III

CHAPTER XV

INEQUALITIES

In this chapter we are concerned entirely with real numbers. By definition $a>b$ means that $a-b$ is positive, and $a<b$ means that $a-b$ is negative; the number 0 is neither positive nor negative.

It is sometimes convenient to use such abbreviations as $a \lesseqgtr b \lesseqgtr c$ if $x \gtreqless y$ for $a<b<c$ if $x>y$ and $a>b>c$ if $x<y$.

The rules for the manipulation of inequalities are nearly but not exactly the same as for equations:

If $a \gtreqless b$, then $a+x \gtreqless b+x$ .....(1)

because $(a+x)-(b+x)=a-b$.

If $a \gtreqless b$, then $ax \gtreqless bx$ if $x>0$ and $ax \lesseqgtr bx$ if $x<0$ .....(2)

because $ax-bx=x(a-b)$ and has the same sign as $a-b$ if $x>0$ and the opposite sign if $x<0$.

If $a_r>b_r>0$ for $r=1, 2, \ldots, n$, then $a_1 a_2 \ldots a_n > b_1 b_2 \ldots b_n$ ...(3)

because successive applications of (2) give

$$a_1 a_2 a_3 \ldots a_n > b_1 a_2 a_3 \ldots a_n > b_1 b_2 a_3 \ldots a_n > \ldots > b_1 b_2 b_3 \ldots b_n.$$

An important deduction from (3) is

If $a>b>0$, then $a^n>b^n$ if $n>0$ and $a^n<b^n$ if $n<0$ .....(4)

and this holds for any rational value $\frac{p}{q}$ $(q>0)$ of n if the convention is made that $a^{p/q}$ denotes the positive q^{th} root of a^p.

This convention will be adopted throughout this chapter.

The reader should note carefully the reversal of the inequalities in (2) and (4) when x and n are negative.

Quadratic Inequalities.

Any quadratic inequality $ax^2+2bx+c>0$ can be reduced to one of the forms

(i) $(x-\alpha)(x-\beta)>0$ (ii) $(x-\alpha)(x-\beta)<0$

(iii) $(x-\gamma)^2+\delta^2>0$ (iv) $(x-\gamma)^2+\delta^2<0$

In order that (i) may be true, $x-\alpha$ and $x-\beta$ must have the same sign. This requires that x should lie outside the interval from α to β.

Similarly (ii) requires that x should lie between α and β.

(iii) is true for all values of x except that if $\delta=0$ it is not true for $x=\gamma$. (iv) is never true.

The conditions for $ax^2+2bx+c$ to be *positive for all values of* x are that *either* $a>0$, $ac-b^2>0$ *or* $a=b=0$, $c>0$.

If $a\neq 0$, $ax^2+2bx+c\equiv\{(ax+b)^2+(ac-b^2)\}/a$.

Hence if $a>0$ and $ac-b^2>0$, $ax^2+2bx+c>0$ for all values of x.

If $a>0$ and $ac-b^2\leqslant 0$, $ax^2+2bx+c\leqslant 0$ for $x\geqslant -b/a$.

If $a<0$, $(ax+b)^2+(ac-b^2)$ is positive for all sufficiently large values of x, and for such values $ax^2+2bx+c$ is negative.

If $a=0$, the inequality reduces to $2bx+c>0$ which is not always true unless $b=0$ and $c>0$. Hence the conditions stated are necessary and sufficient.

Example 1. Solve $\dfrac{1}{x-2}>-1$

If $x-2>0$, the inequality gives

$$1>-x+2, \text{ i.e. } x>1,$$

and so it is true for $x>2$.

If $x-2<0$, it similarly gives $x<1$, and so it is true for $x<1$ as well as for $x>2$.

This result should be illustrated by the graph of $y(x-2)=1$. The inequality might alternatively be written in the form

$$(x-2)^2\{1/(x-2)+1\}>0$$

and solved as a quadratic inequality.

Sets. A *set* of numbers $a_1, a_2, \ldots, a_n$ is denoted by $[a]$.

Two sets $[a]$, $[b]$ such that $a_1 : b_1 = a_2 : b_2 = \ldots = a_n : b_n$ are called *proportional*. This implies that they are proportional when $a_1 = a_2 = \ldots = a_n = 0$ or $b_1 = b_2 = \ldots = b_n = 0$.

A set $[a]$ in which $a_1 = a_2 = \ldots = a_n$ is called a *dull* set.

Weierstrass' Inequalities. Suppose that $a_\nu (\nu = 1, 2, \ldots, n)$ are positive numbers whose sum is s. Then we shall prove that

$$(1+a_1)(1+a_2)\ldots(1+a_n) > 1+s \quad \ldots\ldots(5)$$

$$(1-a_1)(1-a_2)\ldots(1-a_n) > 1-s \text{ if } a_\nu < 1 \quad \ldots\ldots(6)$$

$$(1+a_1)(1+a_2)\ldots(1+a_n) < \frac{1}{1-s} \text{ if } s<1 \quad \ldots\ldots(7)$$

$$(1-a_1)(1-a_2)\ldots(1-a_n) < \frac{1}{1+s} \quad \ldots\ldots(8)$$

Since $(1+a_1)(1+a_2) = 1 + (a_1+a_2) + a_1 a_2 > 1 + (a_1+a_2)$,

$(1+a_1)(1+a_2)(1+a_3) > \{1 + (a_1+a_2)\}(1+a_3) > 1 + (a_1+a_2+a_3)$,

and so on; this proves (5).

Since $(1-a_1)(1-a_2) = 1 - (a_1+a_2) + a_1 a_2 > 1 - (a_1+a_2)$,

it follows from $0 < a_3 < 1$ that

$$(1-a_1)(1-a_2)(1-a_3) > \{1-(a_1+a_2)\}(1-a_3) > 1-(a_1+a_2+a_3);$$

hence if $a_1, a_2, \ldots, a_n$ lie between 0 and 1,

$$(1-a_1)(1-a_2)\ldots(1-a_n) > 1-(a_1+a_2+\ldots+a_n),$$

which proves (6).

From $(1-a_\nu)(1+a_\nu) = 1 - a_\nu^2 < 1$ and $a_\nu < 1$ it follows that $1+a_\nu < 1/(1-a_\nu)$ and therefore

$$(1+a_1)(1+a_2)\ldots(1+a_n) < 1/\{(1-a_1)(1-a_2)\ldots(1-a_n)\}.$$

Also from (6) provided that $s<1$ it follows that

$$1/\{(1-a_1)(1-a_2)\ldots(1-a_n)\} < 1/(1-s)$$

which proves (7).

Similarly (8) can be proved by using (5) and $1-a_\nu < 1/(1+a_\nu)$.

Cauchy's Inequality. *If the sets* $[a]$, $[b]$ *are not proportional,*

$$(a_1b_1+a_2b_2+\ldots+a_nb_n)^2<(a_1^2+a_2^2+\ldots+a_n^2)(b_1^2+b_2^2+\ldots+b_n^2) \quad \ldots(9)$$

Consider the expression $\sum(a_\nu x+b_\nu)^2$. A value of x such that $a_\nu x+b_\nu$ is zero for all the values of ν only exists if the sets are proportional.

Hence $\sum(a_\nu x+b_\nu)^2$, i.e. $x^2\sum a_\nu^2+2x\sum a_\nu b_\nu+\sum b_\nu^2$, is positive for all values of x. Also $\sum a_\nu^2>0$. Therefore by p. 368,

$$\sum a_\nu^2\sum b_\nu^2-(\sum a_\nu b_\nu)^2>0,$$

which proves (9).

Alternatively this result follows from the identity

$$\begin{vmatrix} \sum a_\nu^2 & \sum a_\nu b_\nu \\ \sum a_\nu b_\nu & \sum b_\nu^2 \end{vmatrix} = \tfrac{1}{2}\sum_{\mu=1}^{n}\sum_{\nu=1}^{n}(a_\mu b_\nu-a_\nu b_\mu)^2.$$

If $[a]$, $[b]$ are proportional, the sign $<$ must be replaced by $=$ in the above result.

Tchebychef's Inequality

If $$a_1\geqslant a_2\geqslant\ldots\geqslant a_n \quad \text{and} \quad b_1\geqslant b_2\geqslant\ldots\geqslant b_n$$

then

$$\frac{a_1+a_2+\ldots+a_n}{n}\cdot\frac{b_1+b_2+\ldots+b_n}{n}<\frac{a_1b_1+a_2b_2+\ldots+a_nb_n}{n} \quad \ldots(10)$$

unless $[a]$ or $[b]$ is a dull set.

For if each summation is from 1 to n

$$\sum_\mu\sum_\nu(a_\mu b_\mu-a_\mu b_\nu)=\sum_\mu(na_\mu b_\mu-a_\mu\sum b)=n\sum ab-\sum a\sum b$$

and $$\sum_\mu\sum_\nu(a_\nu b_\nu-a_\nu b_\mu)=\sum_\nu(na_\nu b_\nu-a_\nu\sum b)=n\sum ab-\sum a\sum b.$$

Hence $$n\sum ab-\sum a\sum b=\tfrac{1}{2}\sum_\mu\sum_\nu(a_\mu b_\mu-a_\mu b_\nu+a_\nu b_\nu-a_\nu b_\mu)$$

$$=\tfrac{1}{2}\sum_\mu\sum_\nu(a_\mu-a_\nu)(b_\mu-b_\nu).$$

But by hypothesis $(a_\mu-a_\nu)(b_\mu-b_\nu)$ is positive unless one factor is zero. And in the double sum the terms are not all zero unless $a_1=a_2=\ldots=a_n$ or $b_1=b_2=\ldots=b_n$.

Hence $n\sum ab-\sum a\sum b$ is positive, which proves (10).

In this result, if one of the sets $[a]$, $[b]$ is dull, the inequality is replaced by an equality.

By repeated applications of (10) if

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n, \quad b_1 \geqslant b_2 \geqslant \ldots \geqslant b_n, \ldots, \quad l_1 \geqslant l_2 \geqslant \ldots \geqslant l_n,$$

$$\frac{\sum a}{n}\frac{\sum b}{n}\cdots\frac{\sum l}{n} \leqslant \frac{\sum ab\ldots l}{n} \qquad \ldots\ldots\ldots\ldots(11)$$

provided that at least two of the sets $[a]$, $[b]$, ... , $[l]$ are not dull.

A useful special case of this inequality is obtained by taking the sets

$$a_1^p, a_2^p, \ldots, a_n^p; \quad a_1^q, a_2^q, \ldots, a_n^q; \quad a_1^r, a_2^r, \ldots, a_n^r; \ \ldots$$

of *positive* numbers, where p, q, r, ... have the *same* signs and $p+q+r+\ldots=m$. From these conditions it follows that if $a_1^p, a_2^p, \ldots, a_n^p$ are in descending order of magnitude, so also are the other sets. Hence

$$\frac{\sum a^p}{n}\frac{\sum a^q}{n}\frac{\sum a^r}{n}\cdots \leqslant \frac{\sum a^m}{n} \qquad \ldots\ldots\ldots\ldots(12)$$

unless $[a]$ is a dull set. The form of this result shows that the order in which $a_1, a_2, \ldots, a_n$ are arranged is immaterial.

Example 2. If a, b, c are positive and not all equal and n is a positive integer, prove that $(a+b+c)^n < 3^{n-1}(a^n+b^n+c^n)$.

By formula (11)

$$\frac{a+b+c}{3}\frac{a+b+c}{3}\frac{a+b+c}{3}\ldots n \text{ factors} < \frac{a^n+b^n+c^n}{3}$$

and so $$(a+b+c)^n < 3^{n-1}(a^n+b^n+c^n).$$

EXERCISE XVa

A

Solve the inequalities in Nos. 1-4.

1. $\dfrac{1}{1-x} < \dfrac{1}{x-2}$

2. $-1 < \dfrac{3x+4}{x-7} < 1$

3. $x(1-x) < 1$

4. $x(x-\alpha)(x-\beta) < 0$, $(\alpha < 0 < \beta)$.

5. Find the conditions for $ax^2+2bx+c$ to be negative for all values of x.

6. If $a>0$, $b>0$, $a+b=1$, prove that

(i) $4ab<1$; (ii) $\left(a+\frac{1}{a}\right)^2+\left(b+\frac{1}{b}\right)^2>12\frac{1}{2}$

Prove the inequalities in Nos. 7-11, given that a, b, ... are positive and not all equal.

7. $a^3b+ab^3<a^4+b^4$

8. $(a^4+b^4)(a^5+b^5)<2(a^9+b^9)$

9. $(a+b)^n<2^{n-1}(a^n+b^n)$, where n is a positive integer.

10. $(a^2+b^2+c^2)^2<(a+b+c)(a^3+b^3+c^3)$

11. (i) $(b+c-a)(c+a-b)\leqslant c^2$;
(ii) $(b+c-a)(c+a-b)(a+b-c)<abc$.

12. If x, y, z are positive variables with a constant sum k, find the least value of $x^2+y^2+z^2$.

B

Solve the inequalities in Nos. 13-20.

13. $3-5x<2x-11$

14. $x^2-5x+6<0$

15. $83-8x^3<8-5x^2$

16. $x(x-3)>10$

17. $-1<\frac{2+x}{3-x}<1$

18. $\frac{1}{3x^2-5}>4$

19. $x^2+5<2x$

20. $x^3+1<x^2+x$

21. Under what circumstances is

(i) $x^3+y^3>x^2y+xy^2$; (ii) $(1+xy)^2<(x+y)^2$?

22. Express the following so that only positive signs occur. Also state the conditions for the omission of the equality signs.

(i) If $a>0$, $b>0$, then $(\sqrt{a}-\sqrt{b})^2\geqslant 0$;

(ii) $(b-c)^2+(c-a)^2+(a-b)^2\geqslant 0$;

(iii) $\Sigma\Sigma(a_r-a_s)^2\geqslant 0$, where the summation extends to all possible pairs of values of r and s selected from $1, 2, \ldots, n$.

23. If $x>0$, prove that $2\leqslant x+\frac{1}{x}\leqslant x^3+\frac{1}{x^3}$

24. Prove that $(a/x)^2+(bx)^2>2ab$ unless $bx^2=a$, and find the least value of $cx+d/x$ where c, d, x are positive and c, d are constant.

Prove the inequalities in Nos. 25-30, given that $a, b, \ldots$ are positive and not all equal.

25. $cd(a+b)^2 < (ad+bc)(ac+bd)$

26. $(a^2+b^2)(a^3+b^3)(a^6+b^6) < 4(a^{11}+b^{11})$

27. $(a+b+c+d)^3 < 16(a^3+b^3+c^3+d^3)$

28. $(a+b+c)^2 > 3(bc+ca+ab)$

29. $(a^2+b^2+c^2+d^2)(a^3+b^3+c^3+d^3) < 4(a^5+b^5+c^5+d^5)$

30. $(a+b-c)^2 > 4(ab-bc-ca)$

C

31. If $s_n = a^n + b^n + \ldots + l^n$ and $a, b, \ldots, l$ are positive and not all equal, prove that $s_4 s_5 < s_3 s_6$.

32. If $n-1$ is a positive integer, prove that

$$\frac{3n-1}{2n} < \left(1+\frac{1}{n^3}\right)\left(1+\frac{2}{n^3}\right)\ldots\left(1+\frac{n-1}{n^3}\right) < \frac{2n}{n+1}$$

33. If $0 < x < \frac{1}{2}$, prove that

$$(1+x)(1+x^2)\ldots(1+x^{n-1}) < (1-x)/(1-2x+x^n)$$

34. Prove that $\dfrac{4.7.10\ldots(3n+4)}{2.5.\ 8\ldots(3n+2)} > 1 + \frac{2}{3}\left\{1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n+1}\right\}$

Prove the inequalities in Nos. 35, 36, given that a, b, c are positive and not all equal.

35. $bc(b+c)+ca(c+a)+ab(a+b) < 2(a^3+b^3+c^3)$

36. $(bc+ca+ab)(a+b+c)^4 < 27(a^3+b^3+c^3)^2$

37. Prove that if $a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots$ are all positive,
$(a_1b_1c_1+\ldots+a_nb_nc_n)^3 < (a_1^3+\ldots+a_n^3)(b_1^3+\ldots+b_n^3)(c_1^3+\ldots+c_n^3)$.

38. By arranging s, $\equiv ax^2+2hxy+by^2+2gx+2fy+c$, as a quadratic in x and using the results on p. 368, prove that s is positive for all values of x and y if and only if

(i) $a>0$, $\begin{vmatrix} a & h \\ h & b \end{vmatrix} > 0$, $\begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix} > 0$,

or (ii) $a>0$, $ab-h^2 = gh-af = 0$, $ac-g^2 > 0$,

or (iii) $a=h=g=0$, $b>0$, $bc-f^2>0$,

or (iv) $a=b=f=g=h=0$, $c>0$.

39. If a, b, c are positive and $x+y+z=0$, prove that

$$a^2x^2+b^2y^2+c^2z^2-2bcyz-2cazx-2abxy>0.$$

Illustrate this result geometrically, x, y, z being areal coordinates.

Arithmetic and Geometric Means. We shall now consider certain theorems which are generalisations of the inequality

$$x^2+y^2>2xy.$$

If a, b are positive and unequal, this inequality may be written

$$\frac{a+b}{2}>\sqrt{(ab)}$$

i.e. the arithmetic mean of two unequal positive numbers is greater than the geometric mean.

It will be shown that the same is true of the means of n positive numbers.

The *arithmetic mean* of a set $[a]$ of n positive numbers is the number which is often called their average; it is defined to be $\frac{a_1+a_2+\ldots+a_n}{n}$ and is denoted by $\mathrm{A}(a)$; the *geometric mean* is defined to be $\sqrt[n]{(a_1a_2\ldots a_n)}$ and is denoted by $\mathrm{G}(a)$.

Example 3. If $a_1, a_2, \ldots, a_n$ are unequal positive numbers in A.P., prove that $\sqrt{(a_1a_n)}<\sqrt[n]{(a_1a_2\ldots a_n)}<\frac{1}{2}(a_1+a_n)$.

(i) If b is the common difference, and $0<k<n-1$,

$$\begin{aligned}a_{k+1}a_{n-k}&=(a_1+kb)\{a_1+(n-k-1)b\}\\&>a_1^2+(n-1)a_1b=a_1a_n.\end{aligned}$$

Put $k=1, 2, \ldots, n-2$ and multiply, thus

$$\begin{aligned}a_2^2a_3^2\ldots a_{n-1}^2&>(a_1a_n)^{n-2}\\\therefore\ a_1^2a_2^2\ldots a_n^2&>(a_1a_n)^n\\\therefore\ \sqrt[n]{(a_1a_2\ldots a_n)}&>\sqrt{(a_1a_n)}\end{aligned}$$

(ii) $a_1+a_n=a_{k+1}+a_{n-k}>2\sqrt{(a_{k+1}a_{n-k})}$.

Put $k=0, 1, \ldots, n-1$ and multiply, thus

$$\begin{aligned}(a_1+a_n)^n&>2^n\sqrt{(a_1^2a_2^2\ldots a_n^2)}=2^na_1a_2\ldots a_n\\\therefore\ \tfrac{1}{2}(a_1+a_n)&>\sqrt[n]{(a_1a_2\ldots a_n)}\end{aligned}$$

This is a special case of a result now to be proved.

In the remainder of this chapter we shall be dealing with sets in which all the numbers are positive. The inclusion of zero values often gives rise to exceptional cases the details of which must be left for a more advanced course. [See Hardy, Littlewood and Pólya: *Inequalities*]

Theorem of Means. $A(a) > G(a)$, unless $[a]$ is a dull set. .....(13)

Let a_μ, a_ν be the greatest and least (or one of the greatest and one of the least) terms of $[a]$ and denote by $[b]$ the set obtained from $[a]$ by replacing a_μ, a_ν by G and $a_\mu a_\nu/G$, where $G \equiv G(a)$.

Then $a_1 a_2 \dots a_n = b_1 b_2 \dots b_n$; $\therefore\ G(b) = G(a) = G$

Also $$G + a_\mu a_\nu/G - a_\mu - a_\nu = \{G^2 - G(a_\mu + a_\nu) + a_\mu a_\nu\}/G$$
$$= -(a_\mu - G)(G - a_\nu)/G.$$

But as $[a]$ is not dull, $a_\mu > G$ and $G > a_\nu$

$$\therefore\ G + a_\mu a_\nu/G < a_\mu + a_\nu$$

$\therefore\ b_1 + b_2 + \dots + b_n < a_1 + a_2 + \dots + a_n$. Thus $A(b) < A(a)$.

Similarly a set $[c]$ can be obtained from $[b]$ such that

$$G(c) = G(b) = G \quad \text{and} \quad A(c) < A(b) < A(a).$$

Continuing this process, after $n-1$ steps at most a set is obtained each of whose terms is G, and the arithmetic mean of this set is less than $A(a)$. Hence $G < A(a)$.

When $[a]$ is a dull set, $A(a) = G(a)$.

Weighted Means. More general types of mean are defined by

$$A(a, p) = (p_1 a_1 + p_2 a_2 + \dots + p_n a_n)/P_n$$
$$G(a, p) = (a_1^{p_1} a_2^{p_2} \dots a_n^{p_n})^{1/P_n}$$

where $P_n = p_1 + p_2 + \dots + p_n$, and $p_1, p_2, \dots, p_n$ are positive rational numbers called the *weights* associated with $a_1, a_2, \dots, a_n$.

If the weights are positive integers, $A(a, p)$ and $G(a, p)$ are the ordinary arithmetic and geometric means of a set consisting of p_1 numbers equal to a_1, p_2 numbers equal to a_2, ..., and p_n numbers equal to a_n. Hence by the theorem of means $A(a, p) > G(a, p)$ unless $[a]$ is a dull set.

If the weights are any positive rational numbers, an integer k exists such that $kp_1, kp_2, \ldots, kp_n$ are all positive integers. Denote them by $q_1, q_2, \ldots, q_n$ and put $q_1 + q_2 + \ldots + q_n = Q_n$.

Then $\quad A(a, p) = (\Sigma p_r a_r)/P_n = (\Sigma q_r a_r)/Q_n$

and $\quad G(a, p) = (\Pi a_r^{p_r})^{1/P_n} = (\Pi a_r^{q_r})^{1/Q_n}$

Hence, by what has just been proved, unless $[a]$ is a dull set,

$$A(a, p) > G(a, p) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (14)$$

where $p_1, p_2, \ldots, p_n$ are any positive rational numbers.

In particular, *if* $\alpha, \beta, \ldots, \lambda$ *are* r *positive rational numbers whose sum is unity and if* $a, b, \ldots, l$ *are positive,*

$$\alpha a + \beta b + \ldots + \lambda l > a^\alpha b^\beta \ldots l^\lambda \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (15)$$

unless $a, b, \ldots, l$ are all equal.

It is convenient at this stage to introduce the more general means defined by

$$M_r(a) = \{(a_1^r + a_2^r + \ldots + a_n^r)/n\}^{\frac{1}{r}}$$

$$M_r(a, p) = \{(p_1 a_1^r + p_2 a_2^r + \ldots + p_n a_n^r)/P_n\}^{\frac{1}{r}}$$

where $P_n = p_1 + p_2 + \ldots + p_n$ and $r \neq 0$.

$$M_1(a) \equiv A(a) \quad \text{and} \quad M_1(a, p) \equiv A(a, p)$$

It can be proved that $\lim_{r \to 0} M_r(a) = G(a)$. See Exercise XVc, No. 21.

We do not discuss properties of irrational numbers in this volume, but it may be mentioned that a special difficulty arises in extending inequalities to irrational values of the argument because in taking a limit the sign $<$ becomes $\leqslant$.

Example 4. If $3x + 5y = 2$ and x is positive, find the greatest value of x^3y^2.

By formula (14), if x, y are positive,

$$\sqrt[5]{\{(\tfrac{3}{3}x)^3(\tfrac{5}{2}y)^2\}} < \tfrac{1}{5}(3x + 5y) = \tfrac{2}{5}$$

unless $\frac{3}{3}x = \frac{5}{2}y$ when the expressions are equal. Hence the greatest value of x^3y^2 if x and y are positive is $(\frac{2}{5})^5(\frac{2}{3})^3(\frac{2}{5})^2$, i.e. $2^7 . 3 . 5^{-6}$.

But x^3y^2 is negative when y is negative and hence $2^7 . 3 . 5^{-6}$ is the required greatest value.

Example 5. If a, b, c are positive and not all equal, prove that

$$9a^2b^2c^2 < (bc+ca+ab)(a^4+b^4+c^4).$$

By the theorem of means

$$\tfrac{1}{3}(bc+ca+ab) > \sqrt[3]{(bc.ca.ab)} = \sqrt[3]{(a^2b^2c^2)}$$

and $$\tfrac{1}{3}(a^4+b^4+c^4) > \sqrt[3]{(a^4b^4c^4)};$$

hence $$(bc+ca+ab)(a^4+b^4+c^4) > 9\sqrt[3]{(a^6b^6c^6)} = 9a^2b^2c^2$$

Example 6. If $0<n<m$, prove that

$$m^{2m} < (m+n)^{m+n}(m-n)^{m-n} < \left(m+\frac{n^2}{m}\right)^{2m}.$$

By formula (14) with $1/(m+n)$ and $1/(m-n)$ for a_1 and a_2

$$\left\{\frac{1}{(m+n)^{m+n}}\,\frac{1}{(m-n)^{m-n}}\right\}^{\frac{1}{2m}} < \frac{1+1}{m+n+m-n} = \frac{1}{m},$$

hence $$m^{2m} < (m+n)^{m+n}(m-n)^{m-n}.$$

Again by formula (14),

$$\{(m+n)^{m+n}(m-n)^{m-n}\}^{\frac{1}{2m}} < \frac{(m+n)^2+(m-n)^2}{m+n+m-n} = \frac{m^2+n^2}{m}$$

hence $$(m+n)^{m+n}(m-n)^{m-n} < (m+n^2/m)^{2m}.$$

Example 7. If s is the sum of a set $a_1, a_2, \ldots, a_n$ of positive numbers, prove that unless the set is dull,

$$(n-1)\sum_{\nu=1}^{n}\frac{1}{s-a_\nu} < \sum_{\nu=1}^{n}\frac{1}{a_\nu}$$

Let $b_1, b_2, \ldots, b_{n-1}$ be positive and not all equal.

Then $$b_1+b_2+\ldots+b_{n-1} > (n-1)(b_1b_2\ldots b_{n-1})^{1/(n-1)}$$

and $$\frac{1}{b_1}+\frac{1}{b_2}+\ldots+\frac{1}{b_{n-1}} > (n-1)(b_1b_2\ldots b_{n-1})^{-1/(n-1)}$$

Hence $$(b_1+b_2+\ldots+b_{n-1})\sum_{\nu=1}^{n-1}\frac{1}{b_\nu} > (n-1)^2$$

$$\therefore \sum_{\nu=1}^{n-1}\frac{1}{b_\nu} > \frac{(n-1)^2}{b_1+b_2+\ldots+b_{n-1}}.$$

If $[b]$ is a dull set, this inequality is replaced by an equality.

Let $[b]$ be replaced in turn by each of the n sets formed from $[a]$ by omitting one term, and add the n results. Since $[a]$ is not dull, the inequality holds in at least one case. Hence

$$(n-1)\sum_1^n\frac{1}{a_\nu} > \sum_1^n\frac{(n-1)^2}{s-a_\nu}$$

which proves the required inequality.

EXERCISE XVb

A

1. Find the least value of x^4+y^4 when $x^3+y^3=c^3$.

2. Find the greatest value of x^2y^5 when $x^3+y^3=1$.

Prove the inequalities in Nos. 3-9, given that $a, b, \ldots$ are positive and not all equal.

3. $27abc<(a+b+c)^3$

4. $8abc<(b+c)(c+a)(a+b)$

5. $9abc<(a+b+c)(bc+ca+ab)$

6. $81abcd<(s-a)(s-b)(s-c)(s-d)$ where $s=a+b+c+d$.

7. $\dfrac{9}{a+b+c}<\dfrac{2}{b+c}+\dfrac{2}{c+a}+\dfrac{2}{a+b}<\dfrac{1}{a}+\dfrac{1}{b}+\dfrac{1}{c}$

8. $a+b+c\leqslant ad^{b-c}+bd^{c-a}+cd^{a-b}$

9. $a^cb^d(c+d)^{c+d}\leqslant c^cd^d(a+b)^{c+d}$

10. If $n-1$ is a positive integer, prove that

$$\tfrac{1}{2}(n+1)<(1^1 2^2 3^3 \ldots n^n)^{2/(n^2+n)}<\tfrac{1}{3}(2n+1)$$

B

11. Find the greatest value of $12x^2(1-3x^2)$.

12. Find the least value of $x^{-3}+y^{-3}$ when $x^3+y^3=c^3$.

13. Find the greatest value of x^2y^3 when $x>0$ and $5x+6y=7$.

Prove the inequalities in Nos. 14-20, given that $a, b, \ldots$ are positive and not all equal.

14. $(\sqrt{a}+\sqrt{b}+\sqrt{c})\sqrt{d}+\sqrt{(bc)}+\sqrt{(ca)}+\sqrt{(ab)}<\frac{3}{2}(a+b+c+d)$

15. $25abcde<(a^2+b^2+c^2+d^2+e^2)(a^3+b^3+c^3+d^3+e^3)$

16. $\dfrac{a}{b}+\dfrac{b}{c}+\dfrac{c}{d}+\dfrac{d}{a}>4$

17. $16abcd<(a^3+b^3+c^3+d^3)^3$

18. $\left(\dfrac{a}{e}+\dfrac{b}{f}+\dfrac{c}{g}\right)\left(\dfrac{e}{a}+\dfrac{f}{b}+\dfrac{g}{c}\right)\geqslant 9.$

19. $a^ab^b(a+b)^{a+b}<(a^a+b^b)^{a+b}$

20. $n^n(p-a_1)(p-a_2)\ldots(p-a_n)<p^n$ where

$$p=(a_1+a_2+\ldots+a_n)/(n-1)>a_r \quad (r=1 \text{ to } n).$$

21. If n is a positive integer and $x>0$, $x\neq 1$, prove that

$$(x^{n+1}-1)/(x-1)>(n+1)x^{n/2}.$$

22. If $a_1 > a_2 > \ldots > a_{n+1}$, prove that

$$(a_1 - a_{n+1})^n > n^n (a_1 - a_2)(a_2 - a_3) \ldots (a_n - a_{n+1})$$

unless $a_1, a_2, \ldots, a_{n+1}$ are in A.P.

23. If x, y are positive, prove that $\{\frac{1}{2}(x+y)\}^{x+y} < x^x y^y$.

C

24. Find the least value of $yz + zx + xy$ if $xyz = c^2(x+y+z)$ and x, y, z have the same sign.

25. If n is a positive integer, prove that

$$\sqrt{n} < \sqrt[n]{n!} < \tfrac{1}{2}(n+1)$$

26. If $n-1$ is a positive integer, prove that

(i) $n^n > 1.3.5 \ldots (2n-1)$, (ii) $(n!)^2 < n^n \{\frac{1}{2}(n+1)\}^{2n}$

Prove the inequalities in Nos. 27, 28 given that $a_1, a_2, \ldots, a_n$ are positive and not all equal and that s is their sum.

27. (i) $\sum_1^n \frac{s}{s-a_r} > \frac{n^2}{n-1}$, (ii) $\sum_1^n \frac{a_r}{s-a_r} > \frac{n}{n-1}$

28. $\left(\frac{s}{a_1} - 1\right)^{a_1} \left(\frac{s}{a_2} - 1\right)^{a_2} \ldots \left(\frac{s}{a_n} - 1\right)^{a_n} < (n-1)^s$.

29. If $a_1, a_2, \ldots, a_n$ are unequal positive numbers in A.P., prove that $\frac{2n}{a_1 + a_n} < \sum_1^n \frac{1}{a_r} < \frac{1}{2}n\left(\frac{1}{a_1} + \frac{1}{a_n}\right)$

30. If $n-1$ is a positive integer, prove that

$$\frac{1}{2\sqrt{n}} < \frac{1.3 \ldots (2n-1)}{2.4 \ldots (2n)} < \frac{1}{\sqrt{(2n+1)}}$$

31. If $(x_1 - a)(x_2 - a) \ldots (x_n - a) = b^n$ where $0 < a < x_\nu$ for $\nu = 1$ to n, prove that the least value of $x_1 x_2 \ldots x_n$ is $(a+b)^n$

32. If $\alpha + \beta = 1$ and x, y are positive and unequal and if $\alpha \gtrless 1$ or $\alpha < 0$, prove that $x^\alpha y^\beta > \alpha x + \beta y$.

33. If $\alpha > \frac{1}{2}$ and $x + \alpha > 1$, prove that

$$(x - \alpha)(x + \alpha)^{2\alpha - 1} < (x + \alpha - 1)^{2\alpha}$$

34. (i) If $0 < m < n$ and $0 < x$, prove that $\left(1 + \frac{x}{m}\right)^m < \left(1 + \frac{x}{n}\right)^n$

(ii) If $0 < x < m < n$, prove that $\left(1 - \frac{x}{m}\right)^m < \left(1 - \frac{x}{n}\right)^n$

35. If $0 < m < n$ and $0 < y$, $y \neq 1$, prove that

$$n(\sqrt[n]{y} - 1) < m(\sqrt[m]{y} - 1).$$

Holder's Inequality. If $[a]$ and $[b]$ are two sets of n positive numbers which are not proportional, and if $\alpha+\beta=1$, then

$$\Sigma(a_\nu^\alpha b_\nu^\beta)<(\Sigma a_\nu)^\alpha(\Sigma b_\nu)^\beta \text{ if } \alpha \text{ and } \beta \text{ are positive} \quad \ldots\ldots(16)$$

$$\Sigma(a_\nu^\alpha b_\nu^\beta)>(\Sigma a_\nu)^\alpha(\Sigma b_\nu)^\beta \text{ if } \alpha>1 \text{ or if } \alpha<0 \quad \ldots\ldots\ldots(17)$$

where each summation is taken for $\nu=1, 2, \ldots, n$.

(i) First suppose that α and β are positive.

Let $a_1+a_2+\ldots+a_n=A_n$, $b_1+b_2+\ldots+b_n=B_n$.

In (15) take $r=2$ and write a_ν/A_n, b_ν/B_n for a, b.

Thus $$(a_\nu/A_n)^\alpha(b_\nu/B_n)^\beta<\alpha a_\nu/A_n+\beta b_\nu/B_n$$

unless $a_\nu/A_n=b_\nu/B_n$. Adding the results given by $\nu=1, 2, \ldots, n$,

$$\Sigma(a_\nu^\alpha b_\nu^\beta)/(A_n^\alpha B_n^\beta)<\alpha+\beta=1.$$

Hence $$\Sigma(a_\nu^\alpha b_\nu^\beta)<A_n^\alpha B_n^\beta=(\Sigma a_\nu)^\alpha(\Sigma b_\nu)^\beta.$$

If $a_r/A_n=b_r/B_n$ for any particular value of ν, the corresponding inequality is replaced by an identity, but at least one of the inequalities will hold unless $a_\nu/A_n=b_\nu/B_n$ for all values of ν. Hence the inequality in (16) holds unless $[a]$ and $[b]$ are proportional sets.

(ii) Next suppose that $\alpha>1$, which implies $\beta<0$.

Put $\alpha=1/\gamma$ and $\gamma+\delta=1$. This makes γ and δ positive and $\beta/\alpha=(1-\alpha)/\alpha=\gamma-1=-\delta$.

Also put $a_\nu=c_\nu d_\nu$ and $b_\nu=d_\nu^{-\alpha/\beta}$. This makes

$$a_\nu^\alpha b_\nu^\beta=c_\nu^\alpha=c_\nu^{1/\gamma} \quad \text{and} \quad d_\nu=b_\nu^{-\beta/\alpha}=b_\nu^\delta.$$

In (16) write $c_\nu^{1/\gamma}$, $d_\nu^{1/\delta}$, γ, δ for a_ν, b_ν, α, β.

Then $$\Sigma c_\nu d_\nu<(\Sigma c_\nu^{1/\gamma})^\gamma(\Sigma d_\nu^{1/\delta})^\delta$$

i.e. $$\Sigma a_\nu<(\Sigma a_\nu^\alpha b_\nu^\beta)^{1/\alpha}(\Sigma b_\nu)^{-\beta/\alpha}$$

But α is positive $\therefore\ (\Sigma a_\nu)^\alpha(\Sigma b_\nu)^\beta<\Sigma(a_\nu^\alpha b_\nu^\beta)$

By interchanging a, b and interchanging α, β, it follows that (17) also holds for $\beta>1$ which implies $\alpha<0$.

From (16) and (17) by writing a for a^α and b for b^β it follows that if the sets $[a^{1/\alpha}]$ and $[b^{1/\beta}]$ are not proportional and if $\alpha+\beta=1$, then

$$\Sigma(a_\nu b_\nu)<(\Sigma a_\nu^{\frac{1}{\alpha}})^\alpha(\Sigma b_\nu^{\frac{1}{\beta}})^\beta \text{ if } \alpha \text{ and } \beta \text{ are positive} \quad \ldots\ldots(18)$$

$$\Sigma(a_\nu b_\nu)>(\Sigma a_\nu^{\frac{1}{\alpha}})^\alpha(\Sigma b_\nu^{\frac{1}{\beta}})^\beta \text{ if } \alpha>1 \text{ or if } \alpha<0 \quad \ldots\ldots(19)$$

By using the method employed for proving (16) it may be shown that

if $[a]$, $[b]$, ... , $[l]$ denote m sets not all proportional and if $\alpha, \beta, \ldots, \lambda$ are m positive numbers whose sum is unity, then

$$\Sigma(a_\nu^\alpha b_\nu^\beta \ldots l_\nu^\lambda) < (\Sigma a_\nu)^\alpha (\Sigma b_\nu)^\beta \ldots (\Sigma l_\nu)^\lambda \quad \ldots\ldots\ldots\ldots (20)$$

Minkowski's Inequality. *If* $[a]$ *and* $[b]$ *are two sets which are not proportional, each consisting of* n *positive numbers, and if* $s_\nu = a_\nu + b_\nu$ *for* $\nu = 1, 2, \ldots, n$, *then*

$$M_r(s) < M_r(a) + M_r(b) \text{ if } r > 1 \quad \ldots\ldots\ldots\ldots\ldots (21)$$

$$M_r(s) > M_r(a) + M_r(b) \text{ if } r < 1, \ r \neq 0, \quad \ldots\ldots\ldots (22)$$

(i) First suppose $r > 1$.

Let r' be given by $\dfrac{1}{r} + \dfrac{1}{r'} = 1$, and in formula (18) put $\alpha = 1/r$, $\beta = 1/r'$ and $b_\nu = s_\nu^{r/r'}$; then

$$\Sigma(a_\nu s_\nu^{r-1}) \equiv \Sigma(a_\nu s_\nu^{r/r'}) < (\Sigma a_\nu^r)^{1/r} (\Sigma s_\nu^r)^{1/r'}$$

unless $[a]$ and $[s]$ are proportional. Similarly

$$\Sigma(b_\nu s_\nu^{r-1}) < (\Sigma b_\nu^r)^{1/r} (\Sigma s_\nu^r)^{1/r'}$$

unless $[b]$ and $[s]$ are proportional. Hence by addition

$$\Sigma s_\nu^r < \{(\Sigma a_\nu^r)^{1/r} + (\Sigma b_\nu^r)^{1/r}\} (\Sigma s_\nu^r)^{1/r'}$$

unless $[a]$ and $[b]$ are proportional. But $1 - 1/r' = 1/r$.

Thus $$(\Sigma s_\nu^r)^{1/r} < (\Sigma a_\nu^r)^{1/r} + (\Sigma b_\nu^r)^{1/r}.$$

Dividing by $n^{1/r}$, $M_r(s) < M_r(a) + M_r(b)$.

(ii) If $r < 1$, $r \neq 0$, then $1/r > 1$ or $1/r < 0$. Formula (19) therefore gives the opposite inequalities to those used in (i). This proves formula (22).

By repeated applications of Minkowski's inequality, if the sets $[a]$, $[b]$, ... , $[l]$ each consisting of n positive numbers are not all proportional, and if $s_\nu = a_\nu + b_\nu + \ldots + l_\nu$ for $\nu = 1, 2, \ldots, n$, then

$$M_r(s) < M_r(a) + M_r(b) + \ldots + M_r(l) \text{ if } r > 1 \quad \ldots\ldots\ldots\ldots (23)$$

$$M_r(s) > M_r(a) + M_r(b) + \ldots + M_r(l) \text{ if } r < 1, \ r \neq 0 \quad \ldots\ldots (24)$$

The symbol M_r is undefined for $r = 0$. But a convention is often made to take M_0 to mean G because it can be proved that $M_r(a) \to G(a)$ when $r \to 0$. See Exercise XVc, No. 21.

But if in (24) $r \to 0$, it is only possible to infer that

$$G(s) \geqslant G(a) + G(b) + \ldots + G(l).$$

It is however easy to deduce from (14), p. 376, that

$$\mathrm{G}(s) > \mathrm{G}(a) + \mathrm{G}(b) + \ldots + \mathrm{G}(l) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (25)$$

unless the sets $[a]$, $[b]$, ... , $[l]$ are all proportional. For

$$\left(\frac{a_1}{s_1}\right)^{1/n}\left(\frac{a_2}{s_2}\right)^{1/n} \ldots \left(\frac{a_n}{s_n}\right)^{1/n} < \frac{1}{n}\left(\frac{a_1}{s_1} + \frac{a_2}{s_2} + \ldots + \frac{a_n}{s_n}\right)$$

unless $[a]$ and $[s]$ are proportional, and similar inequalities hold for $[b]$, ... , $[l]$. Hence by addition

$$\{G(a) + G(b) + \ldots + G(l)\}/(s_1 s_2 \ldots s_n)^{1/n} < \frac{1}{n}\left(\frac{s_1}{s_1} + \frac{s_2}{s_2} + \ldots + \frac{s_n}{s_n}\right) = 1,$$

unless $[a]$, $[b]$, ... , $[l]$ are all proportional, and this gives the required result.

Example 8. If $0 < r < s$, prove that $M_r(a) < M_s(a)$ unless the set $[a]$ is dull.

In formula (16) put $b_1 = b_2 = \ldots = b_n = 1$; thus since $[a]$ is not dull,

$$\Sigma a_r{}^{\alpha} < (\Sigma a_r)^{\alpha} n^{1-\alpha} \text{ if } 0 < \alpha < 1.$$

Substituting $a_r{}^s$ for a_r and r/s for α,

$$\Sigma a_r{}^r < (\Sigma a_r{}^s)^{r/s} n^{1-r/s}, \quad 0 < r < s.$$

Hence since r is positive

$$\left(\frac{\Sigma a_r{}^r}{n}\right)^{1/r} < \left(\frac{\Sigma a_r{}^s}{n}\right)^{1/s}$$

If $r < s < 0$ or if $r < 0 < s$, then in the proof of Example 8, $\alpha > 1$ or $\alpha < 0$ and therefore the first two inequalities are reversed; but since $r < 0$ the last inequality remains as it is. Hence

$$M_r(a) < M_s(a) \text{ if } r < s, \quad r \neq 0, \quad s \neq 0.$$

EXERCISE XVc

A

1. Verify that $M_{-r}(a) M_r\left(\frac{1}{a}\right) = 1$.

2. Express $M_r(a, p)$ in the form $M_r(b)$.

3. Deduce from formula (15), p. 376, that

$$\sum_1^n \left(a_r{}^{\frac{1}{2}} b_r{}^{\frac{1}{2}}\right) < \left(\sum_1^n a_r\right)^{\frac{1}{2}} \left(\sum_1^n b_r\right)^{\frac{1}{2}}$$

Prove the inequalities in Nos. 4-9 :

4. $(ax^2+by^2)^4<(a^4+b^4)(x^4+y^4)^2$ unless $ay=bx$

5. $(apx+bqy+crz)^3<(a^3+b^3+c^3)(p^3+q^3+r^3)(x^3+y^3+z^3)$ unless $a:b:c=p:q:r=x:y:z$

6. $(x^3+y^3)^3\leqslant 2(x^5+y^5)^3$

7. $(ax^2+by^2+cz^2)(bc+ca+ab)>abc(x+y+z)^2$

8. $\sqrt{\{(x_1+x_2)^2+(y_1+y_2)^2\}}\leqslant\sqrt{(x_1^2+y_1^2)}+\sqrt{(x_2^2+y_2^2)}$.

9. $(a^2x+b^2y+c^2z)^2(y^2z^2+z^2x^2+x^2y^2)>x^2y^2z^2(a^2+b^2+c^2)^2$ unless $ax=by=cz$.

10. If $r>1$, prove that $\sum_1^n(a_r^r b_r^{1-r})>(\sum_1^n a_r)^r(\sum_1^n b_r)^{1-r}$. What happens if (i) $0<r<1$; (ii) $r<0$?

11. If α, β are positive constants whose sum is unity and x, y are variables whose sum is c, show that the greatest value of $a^\alpha x^\beta+b^\alpha y^\beta$ is $(a+b)^\alpha c^\beta$.

12. If the sets $[a]$ and $[b]$ are not proportional, and $r>1$, prove that

$$(\Sigma p_r a_r^r)^{1/r}+(\Sigma p_r b_r^r)^{1/r}>(\Sigma p_r(a_r+b_r)^r)^{1/r}.$$

B

13. Verify that $M_{rs}(a)=\{M_s(a^r)\}^{1/r}$

Prove the inequalities in Nos. 14-18

14. $(a^3x^3+b^3y^3+c^3z^3)^3\leqslant(a^5+b^5+c^5)^3(x^5+y^5+z^5)^3$.

15. $(a^3+b^3+c^3+d^3)^4<4(a^4+b^4+c^4+d^4)^3$ unless $a=b=c=d$.

16. $(a+b)^5\left(\frac{x^6}{a^5}+\frac{y^6}{b^5}\right)>(x+y)^6$

17. $\sqrt{\{(a+x)^2+(b+y)^2+(c+z)^2\}}<\sqrt{(a^2+b^2+c^2)}+\sqrt{(x^2+y^2+z^2)}$

18. $\sqrt[3]{\{(a+x)^3+(b+y)^3+(c+z)^3\}}<\sqrt[3]{(a^3+b^3+c^3)}+\sqrt[3]{(x^3+y^3+z^3)}$ unless $a:b:c=x:y:z$

C

19. If $0<r<s$, prove that $M_r(a,p)<M_s(a,p)$.

20. If $0<r<s<t$, prove that $\{M_s(a)\}^{s-r}<\{M_r(a)\}^{rp}\{M_t(a)\}^{tq}$ where $p:q:1=t-s:s-r:t-r$.

21. Use the relations

$$\log M_r(a)=\frac{1}{r}\log\left(\frac{1}{n}\Sigma a_r^r\right)=\frac{1}{r}\log\left\{1+\frac{r}{n}\Sigma\log a_r+O(r^2)\right\}$$

to verify that $M_r(a)\to G(a)$ when $r\to 0$.

22. If $a>c>0$, $b>d>0$, $ad\neq bc$, $r>1$, prove that

$$(a^r+b^r)^{1/r}-(c^r+d^r)^{1/r}<\{(a-c)^r+(b-d)^r\}^{1/r}.$$

What happens if $r<1$?

23. If $\alpha+\beta=1$, prove that $M_r(ab)\gtrless M_{r/\alpha}(a)M_{r/\beta}(b)$ according as $\alpha\beta r<>0$ unless the sets $[a^{1/\alpha}]$ and $[b^{1/\beta}]$ are proportional.

Calculus Methods. Many inequalities are conveniently derived from the theorem that if $f(x)$ is a one-valued integrable function of x which is positive for $a<x<b$, then the function $\int_a^b f(x)dx$ is also necessarily positive. This method was used on p. 106 to obtain the important inequality

$$u/(1+u)<\log(1+u)<u \text{ where } 1+u>0,\ u\neq 0,$$

or
$$(t-1)/t<\log t<t-1, \text{ if } t>0,\ t\neq 1 \quad \ldots\ldots\ldots\ldots(26)$$

Alternatively if $f'(x)>0$ for $a<x<b$ and if $f(a)>0$, then $f(x)>0$ for $a<x<b$. And more severe inequalities can often be obtained by using the mean value theorem

$$f(x+h)=f(x)+hf'(x)+\tfrac{1}{2}h^2f''(x+\theta h),\ 0<\theta<1,$$

or an extension involving higher derivatives.

If $x>0$, $x\neq 1$, then

$$x^r-1>r(x-1) \text{ if } r>1 \text{ or } r<0 \ldots\ldots\ldots\ldots(27)$$

and
$$x^r-1<r(x-1) \text{ if } 0<r<1 \quad \ldots\ldots\ldots\ldots(28)$$

Let $f(x)\equiv x^r-1-r(x-1)$; then $f'(x)=r(x^{r-1}-1)$.

(i) if $r>1$ or $r<0$, $f'(x)<0$ for $0<x<1$ and $f'(x)>0$ for $x>1$; hence $f(x)$ decreases as x increases from 0 to 1 and increases when x increases beyond 1. Also $f(1)=0$. Thus $f(x)>0$ when $x>0$, $x\neq 1$.

(ii) if $0<r<1$, $f'(x)>0$ for $0<x<1$ and $f'(x)<0$ for $x>1$; hence $f(x)$ increases as x increases from 0 to 1 and decreases when x increases beyond 1.
Thus $f(x)<0$ when $0<x<1$ and when $x>1$.

In (27) writing x^p for x and q for pr,

$$\frac{x^p-1}{p}<\frac{x^q-1}{q} \text{ for } x>0,\ x\neq 1,\ 0<p<q.$$

Alternatively, this may be proved directly by algebraic methods. If n is a positive integer and $x>1$,

$$nx^n>1+x+x^2+\ldots+x^{n-1}=(x^n-1)/(x-1)$$

As $x-1$ is positive, $nx^{n+1}-n>(n+1)x^n-(n+1)$

$$\therefore\ \frac{x^{n+1}-1}{n+1}>\frac{x^n-1}{n}.$$

If $0<x<1$, the first inequality in this proof is reversed, but $x-1$ is negative; hence the result holds as for $x>1$. Repeated applications of it prove $(x^p-1)/p<(x^q-1)/q$ where p, q are positive integers and $p<q$. If p, q are positive rational numbers, a positive integer d exists such that pd, qd are also positive integers. Then $(y^{pd}-1)/(pd)<(y^{qd}-1)/(qd)$; hence, putting $y=\sqrt[d]{x}$, $(x^p-1)/p<(x^q-1)/q$.

In (27), replacing x by x/y, y/x in succession, where x, y are positive and unequal,

$$ry^{r-1}(x-y)<x^r-y^r<rx^{r-1}(x-y) \text{ if } r>1 \text{ or } r<0 \ldots\ldots(29)$$

$$rx^{r-1}(x-y)<x^r-y^r<ry^{r-1}(x-y) \text{ if } 0<r<1 \ldots\ldots\ldots(30)$$

Example 9. If $x>1$ and $r>1$, prove that

$$\tfrac{1}{2}r(r-1)(x-1)^2/x<(x^r-1)-r(x-1)<\tfrac{1}{2}r(r-1)(x-1)^2x^{r-1}$$

By the mean value theorem, since x is positive,

$$x^r\equiv\{1+(x-1)\}^r=1+(x-1)r+\tfrac{1}{2}(x-1)^2r(r-1)\{1+\theta(x-1)\}^{r-2}$$

where $0<\theta<1$.

Since $x>1$, $1<1+\theta(x-1)<x$, and hence, since $r>1$,

$$\{1+\theta(x-1)\}^{r-2}>\{1+\theta(x-1)\}^{r-1}/x>1/x$$

and $$\{1+\theta(x-1)\}^{r-2}<\{1+\theta(x-1)\}^{r-1}<x^{r-1}.$$

Hence the required result follows.

Note. If $0<x<1$ the inequalities are reversed. For the case $0<r<1$, see Exercise XVd, No. 22.

Convex Functions. If for all unequal values of x_1, x_2 in the interval $a \leqslant x \leqslant b$,

$$f\{\tfrac{1}{2}(x_1+x_2)\} < \tfrac{1}{2}\{f(x_1)+f(x_2)\} \quad \ldots\ldots\ldots\ldots\ldots\ldots(31)$$

the function $f(x)$ is said to be *convex* in the interval.

If $f''(x)$ exists and is positive in the interval, the function is necessarily convex.

For suppose that $a \leqslant x_1 < x_2 \leqslant b$ and put

$$\tfrac{1}{2}(x_1+x_2) = X, \quad \tfrac{1}{2}(x_2-x_1) = h.$$

Then by the mean value theorem

$$f(x_1) \equiv f(X-h) = f(X) - hf'(X) + \tfrac{1}{2}h^2 f''(\xi_1)$$

$$f(x_2) \equiv f(X+h) = f(X) + hf'(X) + \tfrac{1}{2}h^2 f''(\xi_2)$$

where $x_1 < \xi_1 < X < \xi_2 < x_2$.

Hence $\quad \tfrac{1}{2}\{f(x_1)+f(x_2)\} = f(X) + \tfrac{1}{2}h^2\{f''(\xi_1)+f''(\xi_2)\}$

which is greater than $f(X)$ because $f''(\xi_1)$, $f''(\xi_2)$ are positive.

This test for a convex function is sufficient but not necessary.

When $-f(x)$ is a convex function, $f(x)$ is called a *concave* function.

Jensen's Inequalities.

If $f(x)$ is convex in an interval $a \leqslant x \leqslant b$, and if $x_1, x_2, \ldots, x_n$ belong to this interval and are not all equal, then

$$f\left\{\frac{1}{n}(x_1+x_2+\ldots+x_n)\right\} < \frac{1}{n}\{f(x_1)+f(x_2)+\ldots+f(x_n)\} \quad \ldots(32)$$

(i) First suppose that $n = 2^m$ where m is a positive integer. Then, since the function is convex,

$$f(x_1)+f(x_2) > 2f\{\tfrac{1}{2}(x_1+x_2)\}, \quad f(x_3)+f(x_4) > 2f\{\tfrac{1}{2}(x_3+x_4)\}$$

and $\quad f\{\tfrac{1}{2}(x_1+x_2)\}+f\{\tfrac{1}{2}(x_3+x_4)\} > 2f\{\tfrac{1}{2}(x_1+x_2+x_3+x_4)\}$.

Hence $\quad f(x_1)+f(x_2)+f(x_3)+f(x_4) > 2^2 f\{\tfrac{1}{2}(x_1+x_2+x_3+x_4)\}$.

By repetitions of this process, it may be proved that

$$f(x_1)+f(x_2)+\ldots+f(x_n) > nf\left\{\frac{1}{n}(x_1+x_2+\ldots+x_n)\right\}$$

where $n = 2^m$.

(ii) Now suppose that the inequality always holds for $n=k$; then it can be shown that it holds for any $k-1$ given numbers $x_1, x_2, \ldots, x_{k-1}$. For, applying the inequality to the k numbers $x_1, x_2, \ldots, x_{k-1}$ and x_k where x_k is the arithmetic mean of $x_1, x_2, \ldots, x_{k-1}$

$$f(x_1)+f(x_2)+\ldots+f(x_k)>kf\left\{\frac{1}{k}(x_1+x_2+\ldots+x_{k-1}+x_k)\right\}=kf(x_k)$$

$$\therefore\ f(x_1)+f(x_2)+\ldots+f(x_{k-1})>(k-1)f(x_k).$$

Hence the inequality holds for any $k-1$ given numbers.

(iii) But it was proved in (i) that the result holds for $n=2^m$; thus it follows by applications of (ii) that it is true for 2^m-1, 2^m-2, 2^m-3, ..., and so it is true for all positive integral values of n.

By using the method of p. 376 it is easy to show that if $p_1, p_2, \ldots, p_n$ are positive and rational and if $f(x)$ is convex in the interval $a\leqslant x\leqslant b$, then

$$f\left(\frac{p_1x_1+p_2x_2+\ldots+p_nx_n}{p_1+p_2+\ldots+p_n}\right)<\frac{p_1f(x_1)+p_2f(x_2)+\ldots+p_nf(x_n)}{p_1+p_2+\ldots+p_n} \quad \ldots(33)$$

where $x_1, x_2, \ldots, x_n$ all belong to the interval and are not all equal.

Formulae (32), (33) are called *Jensen's inequalities*. Many of the inequalities established in this chapter can be deduced from them. See Exercise XVd, Nos. 10, 20.

Example 10. If a_1, a_2, x_1, x_2 are positive and $x_1\neq x_2$, prove that

$$a_1x_1\log x_1+a_2x_2\log x_2>(a_1x_1+a_2x_2)\log\frac{a_1x_1+a_2x_2}{a_1+a_2}.$$

If $\qquad f(x)=x\log x \quad \text{and} \quad x>0,$

$$f'(x)=1+\log x,\quad f''(x)=\frac{1}{x}>0.$$

Hence $f(x)$ is convex and it follows from (33) that

$$\frac{a_1f(x_1)+a_2f(x_2)}{a_1+a_2}>f\left(\frac{a_1x_1+a_2x_2}{a_1+a_2}\right).$$

Hence the required result follows.

Example 11. Prove that $(1+x)^m+(1-x)^m$ cannot be less than 2 if $m>1$, or if $m<0$ and $|x|<1$.

If $m>1$, $t>0$, and $(1-t)^m$ exists, $(1+t)^{m-1}>(1-t)^{m-1}$

$$\therefore \int_0^x m\{(1+t)^{m-1}-(1-t)^{m-1}\}dt>0 \text{ if } x>0.$$

Thus $$(1+x)^m+(1-x)^m-2>0 \text{ if } x>0;$$

and since $(1+x)^m+(1-x)^m$ is unaltered when x is changed to $-x$, the same inequality holds for $x<0$.

If $m<0$ and $0<t<1$, $(1+t)^{m-1}<(1-t)^{m-1}$

$$\therefore m\{(1+t)^{m-1}-(1-t)^{m-1}\}>0.$$

Hence $$\int_0^x m\{(1+t)^{m-1}-(1-t)^{m-1}\}dt>0 \text{ if } 0<x<1.$$

(The integral does not exist if $x\geqslant 1$.)

Hence as before $(1+x)^m+(1-x)^m-2>0$ if $0<x<1$, and by changing x to $-x$ the same inequality holds for $-1<x<0$.

EXERCISE XVd

A

1. If $0<a<b$ and $k>1$, prove that

$$ka^{k-1}<(b^k-a^k)/(b-a)<kb^{k-1}.$$

2. Prove that if $x>0$

$$\text{(i) } \log x<2\sqrt{x}; \quad \text{(ii) } \log x\leqslant n(\sqrt[n]{x}-1).$$

3. If $0<m<1$ and $-1<x$, prove that $(1+x)^m\leqslant 1+mx$, and deduce that $(1+x)^{m-1}>\{1+(1-m)x\}^{-1}$.

4. If $f(x)\equiv xy-\alpha x^{1/\alpha}-\beta y^{1/\beta}$ where $x>0$, $y>0$, $0<\alpha<1$, and $\alpha+\beta=1$, find the value of x for which $\partial f/\partial x$ is zero. Hence prove that $xy\leqslant \alpha x^{1/\alpha}+\beta y^{1/\beta}$.

5. If $x>0$, $x\neq 1$, prove that $n(\sqrt[n]{x}-1)$ decreases as n increases.

6. If $a\neq 0$ and if $0<x<y$ or $x<y<-a^2$, prove that

$$(1+a^2/x)^x<(1+a^2/y)^y$$

7. If $0<m=p/q<1$ where p, q are positive integers, prove that

(i) if p and q are odd, $(1+x)^m+(1-x)^m<2$

(ii) if p is even and q odd, $(1+x)^m+(1-x)^m>2^m$.

8. If $0<x<y$ and $1<a$, prove that

$$(a^x-a^{-x})/x<(a^y-a^{-y})/y.$$

9. Prove that $-\log x$ is convex and use Jensen's inequality to prove that if $[x]$ is not dull

$$(\Sigma p_\nu \log x_\nu)/\Sigma p_\nu<\log(\Sigma p_\nu x_\nu)-\log \Sigma p_\nu$$

where p_ν, x_ν are positive and ν takes the values from 1 to n.

10. Deduce formula (16), p. 380, from the fact that $\log(1+e^x)$ is convex by taking $x_1=\log(a_2/a_1)$, $p_1=\alpha$, $x_2=\log(b_2/b_1)$, $p_2=\beta$, in formula (33), p. 387.

B

11. Prove that (i) $e^x\geqslant 1+x$, (ii) $e^x<1/(1-x)$ if $x<1$.

12. If a and x are positive, prove that $x\log(a/x)\leqslant a/e$

13. (i) If $x>-1$, $x\neq 0$, and either $m<0$ or $1<m$, prove that

$$1+mx<(1+x)^m.$$

(ii) If $x>0$ and either $m<0$ or $1<m<1+1/x$, prove that

$$(1+x)^{m-1}<\{1+(1-m)x\}^{-1}$$

14. If $0<x<y$, prove that $(1+1/y)^{1+y}<(1+1/x)^{1+x}$

15. If $0<m<n$ and $0<b<a$, prove that

$$n(ab)^{n-m}(a^{2m}-b^{2m})<m(a^{2n}-b^{2n})$$

C

16. If $x>1$, prove that

(i) $2(x-1)/(x+1)<\log x<(x^2-1)/2x$

(ii) $2/(2x-1)<\log\{x/(x-1)\}<(2x-1)/\{2x(x-1)\}$

17. If $x>-1$, prove that $x^2>(1+x)\{\log(1+x)\}^2$

18. If $x>1$, prove that $2+x+\log x>\sqrt{(x^2+10x-2)}$

19. If $0<x<y$, prove that $\dfrac{\log(1+y)}{\log y}<\dfrac{\log(1+x)}{\log x}$

Deduce that, if $0<a$ and $0<m<n$, $m\log(1+a^n)<n\log(1+a^m)$ and $(x^n+y^n)^m<(x^m+y^m)^n$.

20. Deduce formula (18) from formula (33) by taking

$$f(x)=x^{1/\alpha},\quad x>0,\quad p_\nu=b_\nu^{1/\beta},\quad p_\nu x_\nu=a_\nu b_\nu$$

21. If $r<-1$ and $0<x$, $x\neq 1$, prove that

$$rx^r(x-1)>x^r-1>r(x-1)$$

and deduce that if $x>1$, $1+x-x^2<x^{-x}<(1-x+x^2)^{-1}$

22. If $0<r<1<x$, prove that

$$\tfrac{1}{2}r(1-r)(x-1)^2x^{-2}<r(x-1)-(x^r-1)<\tfrac{1}{2}r(1-r)(x-1)^2$$

and find the corresponding result for $0<r<1$, $0<x<1$.

MISCELLANEOUS EXAMPLES

EXERCISE XVe

A

1. If a, b, $ax+by$, are constant, prove that x^2+y^2 is least when $x:y=a:b$. Interpret the result geometrically.

2. If $n-5$ is a positive integer, prove that $n!<(\frac{1}{2}n)^n$

3. If $x>0$, $y>0$, $y\neq 1$, prove that

$$(xy+1)^{x+1}>y^x(x+1)^{x+1}$$

4. If x_1, x_2, ..., x_n are positive variables whose sum is a constant k, and m is a given positive integer, find the least value of $x_1^m+x_2^m+\ldots+x_n^m$.

5. If a_1, a_2, a_3, a_4 are positive and not all equal, prove that

$$16a_1a_2a_3a_4<(\Sigma a_r^2)^2<(\Sigma a_r)(\Sigma a_r^3)<4\Sigma a_r^4.$$

6. If a, b, c, d are positive and not all equal, prove that

$$16(a+b+c+d)^{-1}<3\Sigma(b+c+d)^{-1}<\Sigma a^{-1}.$$

7. If $n>0$, $n\neq 1$, prove that $(n+1)^{n+1}<2^{n+1}n^n$.

8. Deduce from Jensen's inequality (32) with $f(x)=\log\sec x$ that $\cos x_1\cos x_2\ldots\cos x_n\leqslant\cos^n\theta$ where

$$0<x_r<\tfrac{1}{2}\pi \quad\text{and}\quad \theta=(x_1+x_2+\ldots+x_n)/n.$$

9. If a, b, c are positive and not all equal, prove that

$$abc(a^3+b^3+c^3)<\sqrt[3]{\{(b^5c^5+c^5a^5+a^5b^5)(a^5+b^5+c^5)^4\}}$$

10. If a, b, c, x, y, z are positive, prove that

$$\{\Sigma\sqrt[3]{(a^3+x^3)^4}\}^3\leqslant\{\sqrt[4]{(a^4+b^4+c^4)^3}+\sqrt[4]{(x^4+y^4+z^4)^3}\}^4$$

B

11. Solve the inequality $x(x-3)(x^2-4)<0$

12. If a, b, c are positive, prove that

$$\frac{bc}{b+c}+\frac{ca}{c+a}+\frac{ab}{a+b}\leqslant\tfrac{1}{2}(a+b+c)$$

13. If $a^2+b^2=4$, prove that $a^4+b^4+a^{-4}+b^{-4}\geqslant 8\frac{1}{2}$

14. Prove that $(a+b)^7 \leqslant 64(a^7+b^7)$

15. If $n-1$ is a positive integer, prove that

$$2^n > 1 + n\sqrt{2^{n-1}}$$

16. Prove that $(a^8+b^8)(a^3+b^3) \leqslant 2(a^5+b^5)$

17. If k and n are unequal positive integers and $k<2n$, prove that

(i) $(n!)^2 < k!(2n-k)!$; (ii) $(n!)^n < 1!\,3!\,5! \ldots (2n-1)!$

18. If a, b, c, d are positive and not all equal, prove that

$$(a^4+b^4+c^4+d^4)(a^3+b^3+c^3+d^3) < 4(a^7+b^7+c^7+d^7)$$

19. If a, b, c are positive and not all equal, prove that

$$a^3+b^3+c^3+15abc < 2(a+b+c)(a^2+b^2+c^2)$$

20. If $x-a_1, x-a_2, \ldots, x-a_n$ are positive and not all equal and $a_1+a_2+\ldots+a_n=na$, prove that

$$\Sigma(x-a_\nu)^{-1} > n(x-a)^{-1}.$$

C

21. If $0<x<1$, prove that

$$(1+x)^{1-x}(1-x)^{1+x} < 1 < (1+x)^{1+x}(1-x)^{1-x}$$

and deduce that if $0<b<a$

$$a^b b^a < \{\tfrac{1}{2}(a+b)\}^{a+b} < a^a b^b$$

22. If $n-1$ is a positive integer, prove that

$$n < \sqrt{\{(n+1)^{1+1/n}(n-1)^{1-1/n}\}} < n + 1/n.$$

23. With the hypothesis of Tchebychef's inequality (10) prove that $\Sigma(p_\nu a_\nu)\Sigma(p_\nu b_\nu) < \Sigma p_\nu \Sigma(p_\nu a_\nu b_\nu)$ where $p_\nu > 0$.

24. If $a_1, a_2, \ldots, a_n$ are positive and not all equal, prove that $(\Sigma a_\nu^m)^s < (\Sigma a_\nu^{m+s})(\Sigma a_\nu^{m-s})$ where $s \neq 0$ and each sum is taken for $\nu = 1, 2, \ldots, n$.

25. Prove that $1+\frac{1}{2}+\frac{1}{3}+\ldots+1/n$ lies between

$$n\{(n+1)^{1/n}-1\} \quad \text{and} \quad n\{1+(n+1)^{-1}-(n+1)^{-1/n}\}$$

26. If $n>0$ and $x>1$, prove that

$$n(x^{n+1}-1) > (n+1)(x^n-1)\sqrt{x}$$

27. If $a>0$ and $ab>h^2+k^2$, prove that

$$ax^2+2hxy+by^2+a\xi^2+2h\xi\eta+b\eta^2+2k(x\eta-y\xi) \geqslant 0.$$

28. If $n-1$ is a positive integer and $a_1, a_2, \ldots, a_n$ are positive numbers whose sum is s, prove that

$$(1+a_1)(1+a_2)\ldots(1+a_n) < 1 + \sum_1^n (s^\nu/\nu!).$$

CHAPTER XVI

DETERMINANTS

Permutations. If $a_1, a_2, \ldots, a_n$ are the numbers $1, 2, \ldots, n$ in any order, it is possible to bring them into the ascending order $1, 2, \ldots, n$ by making a finite number of exchanges.

At the first exchange 1 may be brought to the first place; then 2 may be brought to the second place; and so on. Thus after $n-1$ exchanges at most the natural order will be obtained.

For example, starting with 53412 the exchange of 5 and 1 gives 13452 and then the exchange of 3 and 2 gives 12453; continuing in this way two more exchanges give 12354 and then 12345. Often a smaller number than $n-1$ will suffice; for example three exchanges will bring 214365 to 123456.

The number of exchanges depends on the method employed, but it will now be shown that if the number is *even* for one method, it is *even* for every method and if it is *odd* for one method, it is *odd* for every method.

Consider the $\frac{1}{2}n(n-1)$ pairs of numbers such as a_r, a_s in the set $a_1, a_2, \ldots, a_n$. Each such pair must finally be in ascending order.

If in the arrangement

$$a_1, a_2, \ldots, a_{r-1}, a_r, a_{r+1}, \ldots, a_{s-1}, a_s, a_{s+1}, \ldots, a_n,$$

the terms a_r, a_s are exchanged the only pairs whose orders are affected are contained in the terms printed in heavy type and are

$$(a_r, a_{r+1}),\ (a_r, a_{r+2}),\ \ldots,\ (a_r, a_{s-1}),\ (a_r, a_s)$$
$$(a_{r+1}, a_s),\ (a_{r+2}, a_s),\ \ldots,\ (a_{s-1}, a_s).$$

These are $2s-2r-1$ in number. Hence *one* exchange causes an odd number of alterations of order.

If then in the original set $a_1, a_2, \dots, a_n$, an odd number of pairs a_r, a_s have the descending order, the number of exchanges required to produce the necessary alterations must be odd; and if the number of descending pairs is even, the number of exchanges must also be even.

It follows that permutations of **1, 2, ..., n** may be classified as *even permutations* and *odd permutations*.

Similarly any permutation $b_1, b_2, \dots, b_n$ of the set $c_1, c_2, \dots, c_n$ may be classified as an even or odd permutation according as the number of exchanges required to pass from one set to the other is even or odd.

Delta and Epsilon Symbols.

The symbol $\delta^{a_1 a_2 \dots a_n}_{b_1 b_2 \dots b_n}$ is defined to mean

+1, if $a_1 a_2 \dots a_n$ is an even permutation of $b_1 b_2 \dots b_n$

−1, if $a_1 a_2 \dots a_n$ is an odd permutation of $b_1 b_2 \dots b_n$

0, if $a_1 a_2 \dots a_n$ is not a permutation of $b_1 b_2 \dots b_n$

The upper and lower sets $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ are interchangeable and one of them must consist of n different numbers. Thus $\delta^{742}_{274} = +1$, $\delta^{13}_{21} = -1$, $\delta^{23}_{11} = 0$, but δ^{11}_{11} is meaningless.

When one set is 1, 2, 3, ..., n, it is omitted and ϵ is used instead of δ. Thus

$$\delta^{1\ 2\ 3\ \dots\ n}_{a_1 a_2 a_3 \dots a_n} = \delta^{a_1 a_2 a_3 \dots a_n}_{1\ 2\ 3\ \dots\ n} = \epsilon_{a_1 a_2 a_3 \dots a_n}$$

Dummy Suffix Convention. It is often convenient to omit the sign Σ of a summation and to write for example $a_\rho x_\rho$ ($\rho = 1$ to 3) instead of $\sum_{\rho=1}^{3} (a_\rho x_\rho)$ or $a_1 x_1 + a_2 x_2 + a_3 x_3$, or to write $a_{p\alpha} b_{\alpha q}$ ($\alpha = 1$ to n) instead of $\sum_{\alpha=1}^{n} (a_{p\alpha} b_{\alpha q})$ or $a_{p1} b_{1q} + a_{p2} b_{2q} + \dots + a_{pn} b_{nq}$.

The convention is made that if a small *greek* letter occurs as a suffix twice in one term, then that term stands for the sum of its values for all relevant values of the suffix. The relevant

values are stated unless they are obvious from the context. In a sum such as $\epsilon_{\lambda\mu}x_\lambda y_\mu$ it is unnecessary to state the values of λ, μ because $\epsilon_{\lambda\mu}=0$ unless $\lambda=1$, $\mu=2$ or $\lambda=2$, $\mu=1$; thus there are only two non-zero terms in this sum, which is $x_1y_2-x_2y_1$.

A suffix to which the convention applies is called a *dummy suffix* because it can be replaced by any other small *greek* letter that does not occur elsewhere in the term.

The convention applies to double (or multiple) summations when there are two (or more) repeated suffixes present in a single term. Thus $a_{\beta\gamma}x_\beta x_\gamma$ $(\beta=1, 2;\ \gamma=1, 2)$ denotes $a_{11}x_1^2+(a_{12}+a_{21})x_1x_2+a_{22}x_2^2$.

A dummy suffix must not occur more than twice in the same term. A suffix which is not a dummy is called a *free suffix*. For example $x_{\alpha\beta}y_{\beta p}$ contains two free suffixes (α, p) and is the same as $x_{\alpha\gamma}y_{\gamma p}$; also $a_{\mu\nu}b_{\nu\mu}=a_{\nu\mu}b_{\mu\nu}$; but $x_{\mu\nu}y_{\nu\nu}$ is undefined.

Some other obvious abbreviations, such as denoting the set of n equations $x_1=y_1$, $x_2=y_2$, ..., $x_n=y_n$, by $x_\alpha=y_\alpha$ $(\alpha=1$ to $n)$, are also used.

The object of restricting the convention to small greek letters is to make it possible to write down a general term such as a_nx_n, $x_{\alpha n}y_{n\beta}$ or $a_{mn}x_my_n$ without implying a summation. But writers are not agreed about this restriction, and another plan is to use any small letter as a dummy excluding only capital letters from the convention.

The order in which the summation is carried out in such an expression as $a_{\mu\nu}x_\mu x_\nu$ $(\mu=1, 2, 3;\ \nu=1, 2)$ is immaterial:

$$\begin{aligned}(a_{\mu\nu}x_\mu)x_\nu&=(a_{1\nu}x_1+a_{2\nu}x_2+a_{3\nu}x_3)x_\nu\\&=(a_{1\nu}x_\nu)x_1+(a_{2\nu}x_\nu)x_2+(a_{3\nu}x_\nu)x_3\\&=(a_{11}x_1+a_{12}x_2)x_1+(a_{21}x_1+a_{22}x_2)x_2+(a_{31}x_1+a_{32}x_2)x_3\end{aligned}$$

and
$$\begin{aligned}x_\mu(x_\nu a_{\mu\nu})&=x_\mu(x_1a_{\mu1}+x_2a_{\mu2})\\&=x_1(x_\mu a_{\mu1})+x_2(x_\mu a_{\mu2})\\&=x_1(x_1a_{11}+x_2a_{21}+x_3a_{31})+x_2(x_1a_{12}+x_2a_{22}+x_3a_{32})\end{aligned}$$

give the same sum, namely $\sum_\mu\sum_\nu(a_{\mu\nu}x_\mu x_\nu)$. This is further illustrated in the following example.

Example 1. Evaluate $a_\lambda b_{\lambda\mu} c_\mu$ $(\lambda, \mu = 1 \text{ to } 3)$.

This is the sum of nine terms which may be written down by giving to λ, μ the values 1, 1; 1, 2; 1, 3; 2, 1; 2, 2; 2, 3; 3, 1; 3, 2; 3, 3, *in any order.*

The insertion of brackets as in $(a_\lambda b_{\lambda\mu})c_\mu$ or $a_\lambda(b_{\lambda\mu}c_\mu)$ does not affect the nine terms but gives them in a particular order. For example in $a_\lambda b_{\lambda\mu}$ only the λ is a dummy suffix; hence

$$\begin{aligned}(a_\lambda b_{\lambda\mu})c_\mu &= (a_1 b_{1\mu} + a_2 b_{2\mu} + a_3 b_{3\mu})c_\mu \\ &= a_1 b_{1\mu} c_\mu + a_2 b_{2\mu} c_\mu + a_3 b_{3\mu} c_\mu.\end{aligned}$$

μ is now a dummy suffix, and the expression equals

$$\begin{aligned}a_1(b_{11}c_1 + b_{12}c_2 + b_{13}c_3) + a_2(b_{21}c_1 + b_{22}c_2 + b_{23}c_3) \\ + a_3(b_{31}c_1 + b_{32}c_2 + b_{33}c_3).\end{aligned}$$

Similarly $a_\lambda(b_{\lambda\mu}c_\mu)$ gives the equivalent expression

$$\begin{aligned}(a_1 b_{11} + a_2 b_{21} + a_3 b_{31})c_1 + (a_1 b_{12} + a_2 b_{22} + a_3 b_{32})c_2 \\ + (a_1 b_{13} + a_2 b_{23} + a_3 b_{33})c_3.\end{aligned}$$

Example 2. Evaluate $a_{\mu\nu}\delta^\rho_\nu$ $(\nu = 1 \text{ to } n)$.

$$a_{\mu\nu}\delta^\rho_\nu = a_{\mu 1}\delta^\rho_1 + a_{\mu 2}\delta^\rho_2 + \ldots + a_{\mu n}\delta^\rho_n;$$

but by definition $\delta^\rho_\nu = 1$ if $\rho = \nu$ and is otherwise zero; hence the expression is equal to $a_{\mu\rho}$ if ρ is one of the numbers 1 to n, and is otherwise zero.

Example 3. If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are two permutations of $1, 2, \ldots, n$ and if the pairs $(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)$ are rearranged as $(c_1, 1), (c_2, 2), \ldots, (c_n, n)$ and also as $(1, d_1), (2, d_2), \ldots, (n, d_n)$, prove that $\epsilon_{c_1 c_2 \ldots c_n} = \epsilon_{d_1 d_2 \ldots d_n}$.

The value of $\delta^{a_1 a_2 \ldots a_n}_{b_1 b_2 \ldots b_n}$ is unaffected by the simultaneous interchange of a_r, a_s and of b_r, b_s; hence it is unaffected by any identical rearrangement of the upper and lower suffixes; but two such rearrangements give

$$\delta^{c_1 c_2 \ldots c_n}_{1\ 2 \ldots n} \quad \text{and} \quad \delta^{1\ 2 \ldots n}_{d_1 d_2 \ldots d_n}$$

and therefore these are equal. They are equivalent to

$$\epsilon_{c_1 c_2 \ldots c_n} \quad \text{and} \quad \epsilon_{d_1 d_2 \ldots d_n}.$$

EXERCISE XVIa

A

Evaluate the expressions in Nos. 1-6.

1. δ^{1453}_{3214} 2. δ^{23657}_{43572} 3. ϵ_{24631}

4. δ^{abcd}_{dcba} 5. δ^{214}_{212} 6. ϵ_{2345}

Write fully the sums in Nos. 7-10.

7. $x_\alpha x_\alpha$ $(\alpha = 1, 2)$ 8. $a_\lambda b_\lambda$ $(\lambda = 1 \text{ to } 3)$

9. $x_{\alpha\gamma} x_{\gamma\beta}$ $(\gamma = 1 \text{ to } 3)$ 10. $\delta^\mu_\lambda a_{\lambda\nu} a_{\mu\nu}$ $(\lambda, \mu = 1 \text{ to } n)$

Write as determinants the sums in Nos. 11-13.

11. $\delta^{12}_{\alpha\beta} x_\alpha y_\beta$ 12. $a_{\lambda 1} a_{\mu 2} \epsilon_{\lambda\mu}$ 13. $\epsilon_{\lambda\mu\nu} x_\lambda y_\mu z_\nu$

14. Write $a_{1\lambda} a_{2\mu} a_{3\nu} \epsilon_{\lambda\mu\nu}$ as a determinant and verify that it is the same as $a_{1\lambda}(\epsilon_{\lambda\mu\nu} a_{2\mu} a_{3\nu})$.

15. If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are permutations of $1, 2, \ldots, n$, prove that $\delta^{a_1 a_2 \ldots a_n}_{b_1 b_2 \ldots b_n} = \epsilon_{a_1 a_2 \ldots a_n} \epsilon_{b_1 b_2 \ldots b_n}$

16. If x_1, x_2, x_3 are homogeneous coordinates in geometry of two dimensions, state what is represented by :

(i) $a_\rho x_\rho = 0$ $(\rho = 1 \text{ to } 3)$ (ii) $a_\rho / x_\rho = 0$ $(\rho = 1 \text{ to } 3)$

(iii) $a_{\lambda\mu} x_\lambda x_\mu = 0$ $(\lambda, \mu = 1, 2)$.

B

17. Find the number of permutations of 1, 2, 3, 4 which require three exchanges to bring them into the ascending order.

Evaluate the expressions in Nos. 18-20.

18. δ^{142857}_{124578} 19. $\epsilon_{24736851}$ 20. $\epsilon_{\lambda\mu} \epsilon_{\lambda\mu}$

21. If a, b, c, d, e, f is an even permutation of 1, 2, 3, 4, 5, 6, find the values of c, d, e when $c < d < e$ and

(i) $a = 2, b = 5$; (ii) $a = 3, b = 6$; (iii) $a = 4, b = 1$

22. Verify that $\epsilon_{\lambda\mu}(a_{1\alpha} b_{\alpha\lambda})(a_{2\beta} b_{\beta\mu})$ $(\alpha, \beta = 1 \text{ to } 3)$ contains 36 terms half of which are zero. Show that the other 18 terms are also obtained from $(a_{1\alpha} a_{2\beta})(\epsilon_{\lambda\mu} b_{\alpha\lambda} b_{\beta\mu})$ in 9 pairs by evaluating the second bracket with α, β constant and then assigning to α, β the nine possible values.

23. Give the condition for the tangent at y_ρ to the curve $a_\rho x_\rho^2 = 0$ $(\rho = 1 \text{ to } 3)$ to pass through z_ρ. Also give the condition for y_ρ and z_ρ to be conjugate points with respect to this curve.

C

Evaluate the expressions in Nos. 24-27.

24. $\epsilon_{234\ldots n1}$ 25. $\delta^{a_1 a_2 \ldots a_n}_{a_n \ldots a_2 a_1}$

26. $\epsilon_{13\ldots(2n-1)24\ldots(2n)}$ 27. $\epsilon_{\lambda\mu\nu}\epsilon_{\lambda\mu\nu}$

28. Express $\epsilon_{\lambda\mu\nu}\epsilon_{\alpha\beta\gamma}x_{\lambda\alpha}x_{\mu\beta}x_{\nu\gamma}$ as a determinant.

29. Prove that just half of the $n!$ permutations of $1, 2, \ldots, n$ are odd.

30. If $\lambda, \mu = 1$ to 3, interpret the equations

$$\text{(i) } a_{\lambda\mu}x_\lambda x_\mu = 0, \quad \text{(ii) } a_{\lambda\mu}(x_\lambda y_\mu + x_\mu y_\lambda) = 0$$

in terms of homogeneous coordinates x_1, x_2, x_3 in two-dimensional geometry.

31. If two permutations $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ of $1, 2, \ldots, n$ are such that whenever $a_p = q$ then $b_q = p$, prove that they are both even or both odd permutations.

Determinants.

A definition of a determinant of the fourth order was given in Chapter IX, page 183, and it was stated that determinants of higher orders could be defined in succession in a similar way. Denoting the general determinant of order n by

$$\Delta \equiv \begin{vmatrix} a_{11} & a_{12} & a_{13} \ldots a_{1n} \\ a_{21} & a_{22} & a_{23} \ldots a_{2n} \\ \vdots & \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2} & a_{n3} \ldots a_{nn} \end{vmatrix} \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

where the first suffix in a_{pq} corresponds to the *row* in which a_{pq} occurs and the second suffix corresponds to the *column*, and denoting by M_{pq} the determinant obtained by striking out the p^{th} row and the q^{th} column of Δ, the value of Δ may be defined as

$$\sum_{r=1}^{n} (-1)^{r+1} a_{1r} M_{1r}$$

$$\text{or} \quad (-1)^{\nu+1} a_{1\nu} M_{1\nu} \quad (\nu = 1 \text{ to } n) \quad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

In this definition the value of a determinant of order n is defined in terms of the values of determinants of order $n-1$.

But instead of proceeding on these lines, we shall give a self-contained definition and shall make use of the notation explained at the beginning of this chapter.

Consider the array of numbers

$$\begin{matrix} a_{11} & a_{12} & a_{13} \cdots a_{1n} \\ a_{21} & a_{22} & a_{23} \cdots a_{2n} \\ \vdots & \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2} & a_{n3} \cdots a_{nn} \end{matrix}$$

and any particular product of n factors formed by taking one number from each row and also from each column; this term may be written

$$\text{either as } a_{\mu_1 1} a_{\mu_2 2} \cdots a_{\mu_n n} \quad \text{or as } a_{1\nu_1} a_{2\nu_2} \cdots a_{n\nu_n}$$

where $\mu_1, \mu_2, \ldots, \mu_n$ and $\nu_1, \nu_2, \ldots, \nu_n$ are permutations of $1, 2, \ldots, n$.

If the factors $a_{\mu_1 1}, a_{\mu_2 2}, \ldots, a_{\mu_n n}$ are permuted into the order $a_{1\nu_1}, a_{2\nu_2}, \ldots, a_{n\nu_n}$, this permutation puts $\mu_1, \mu_2, \ldots, \mu_n$ into the order $1, 2, \ldots, n$ and at the same time puts $1, 2, \ldots, n$ into the order $\nu_1, \nu_2, \ldots, \nu_n$. Hence

$$\text{if } a_{\mu_1 1} a_{\mu_2 2} \cdots a_{\mu_n n} \equiv a_{1\nu_1} a_{2\nu_2} \cdots a_{n\nu_n}$$

$$\epsilon_{\mu_1 \mu_2 \cdots \mu_n} = \epsilon_{\nu_1 \nu_2 \cdots \nu_n}. \quad \text{(Compare Example 3, p. 395)}$$

There are $n!$ different terms which can be constructed from the given set in this way, and this equality holds for each of them. Therefore the sums

$$\epsilon_{\mu_1 \mu_2 \cdots \mu_n} a_{\mu_1 1} a_{\mu_2 2} \cdots a_{\mu_n n} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$\epsilon_{\nu_1 \nu_2 \cdots \nu_n} a_{1\nu_1} a_{2\nu_2} \cdots a_{n\nu_n} \quad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

are equal. Their value is taken as the definition of the determinant (1) on p. 397, which is also denoted by $|a_{\mu\nu}|$, by $|\alpha|$, or by $(a_{11} a_{22} \cdots a_{nn})$ where the elements given are those of the leading diagonal. To prove the equivalence of the definitions (3) or (4) with (2) it remains to establish the identity of the signs, because each definition gives all the terms composed of elements one from each row and one from each column. This will be done on p. 401. But the fundamental properties proved in Ch. IX for third order determinants will first be established for determinants of order n.

(i) *If the rows of a determinant* $|a_{\mu\nu}|$ *are identical with the columns of* $|b_{\mu\nu}|$ *so that* $a_{\mu\nu} \equiv b_{\nu\mu}$, *then* $|a_{\mu\nu}| = |b_{\mu\nu}|$.

This is implicit in the equality of the sums (3), (4). The value of $|a|$ in the form (3) is identical with that of $|b|$ in the form (4).

It follows that *theorems established for rows hold also for columns, and conversely.*

The determinant obtained from $|a_{\mu\nu}|$ by transposing its rows and columns is called the *transposed* of $|a_{\mu\nu}|$.

(ii) *If two rows (or columns) of a determinant are exchanged, the absolute value of the determinant is unaltered, but its sign is changed.*

For when the r^{th} and s^{th} rows are exchanged, the effect on $\epsilon_{\nu_1 \dots \nu_r \dots \nu_s \dots \nu_n} a_{1\nu_1} a_{2\nu_2} \dots a_{n\nu_n}$ is to replace $a_{r\nu_r}, a_{s\nu_s}$ by $a_{s\nu_r}, a_{r\nu_s}$. Exchange of the dummy suffixes ν_r, ν_s restores the original factors but alters $\epsilon_{\nu_1 \dots \nu_r \dots \nu_s \dots \nu_n}$ into $\epsilon_{\nu_1 \dots \nu_s \dots \nu_r \dots \nu_n}$ and this involves a change of sign, (the consequence of one exchange).

It follows that an *even* permutation of the rows (or columns) of a determinant leaves its value unchanged, and that an *odd* permutation changes its sign.

In other words if after any permutation the p^{th}, q^{th}, r^{th}, ... rows occupy the places of the 1^{st}, 2^{nd}, 3^{rd}, ... rows,

$$|a| \text{ is changed into } \epsilon_{pqr \dots} |a|.$$

But the expression (4) then becomes $\epsilon_{\nu_1 \nu_2 \nu_3 \dots} a_{p\nu_1} a_{q\nu_2} a_{r\nu_3} \dots$

Hence $$\epsilon_{\nu_1 \nu_2 \dots} a_{p\nu_1} a_{q\nu_2} \dots = \epsilon_{pq \dots} |a| \quad \dots\dots\dots\dots\dots (5)$$

Similarly $$\epsilon_{\mu_1 \mu_2 \dots} a_{\mu_1 p} a_{\mu_2 q} \dots = \epsilon_{pq \dots} |a| \quad \dots\dots\dots\dots\dots (6)$$

(iii) *If two rows (or columns) of a determinant are identical, the determinant is zero.*

The exchange of the two rows evidently leaves $|a|$ unaltered. But by (ii) it changes it into $-|a|$. Hence $|a| = 0$.

(iv) *If each element of one row (or column) of a determinant is multiplied by k, the value of the determinant is multiplied by k.*

This follows from the fact that each term contains one and only one factor from each row.

For the same reason a determinant which has a row (or column) of zeros is itself zero.

(v) *If three determinants* $|x|$, $|y|$, $|z|$ *have all their corresponding elements equal except those of the* r^{th} *row (or column), and if each element of the* r^{th} *row (or column) of* $|x|$ *is equal to the sum of the corresponding elements of* $|y|$ *and* $|z|$, *then* $|x|=|y|+|z|$.

If any one of the determinants is written in the form

$$\epsilon_{\nu_1\nu_2\dots\nu_n} a_{1\nu_1} a_{2\nu_2} \dots a_{n\nu_n}$$

the same expression represents the other two except that $x_{r\nu}$, $y_{r\nu}$, $z_{r\nu}$ are written for $a_{r\nu}$ in the values of $|x|$, $|y|$, $|z|$ respectively, where by hypothesis $x_{r\nu}=y_{r\nu}+z_{r\nu}$ and so $|x|=|y|+|z|$.

(vi) *A determinant is unchanged in value by the addition to the elements of one row (or column) of any fixed multiple of the elements of another row (or column).*

This is a consequence of (iii), (iv) and (v).

These results are much used in the practical evaluation of determinants. When repeated use is made of (vi) it is convenient in describing such a process to use the notation

$$\text{row } 2+h \text{ row } 1+k \text{ row } 4$$

to indicate that the elements of the first row multiplied by h and the elements of the fourth row multiplied by k have been added to the elements of the second row.

Similarly, col $3-h$ col $1+k$ col 5 may be used.

Minors and Co-factors. If from the determinant $|a_{\mu\nu}|$ of order n the p^{th} row and q^{th} column are struck out, the remaining elements form a determinant of order $n-1$ which is called the *minor* of a_{pq} and may be denoted by M_{pq}.

Thus $M_{11}\equiv(a_{22}a_{33}\dots a_{nn})=\delta^{2\ 3\ \dots\ n}_{\nu_2\nu_3\dots\nu_n} a_{2\nu_2}a_{3\nu_3}\dots a_{n\nu_n}$

and since $$|a|=\epsilon_{\nu_1\nu_2\dots\nu_n} a_{1\nu_1}a_{2\nu_2}\dots a_{n\nu_n}$$

$$=a_{1\nu_1}\delta^{1\ 2\ \dots\ n}_{\nu_1\nu_2\dots\nu_n} a_{2\nu_2}\dots a_{n\nu_n}$$

the sum of the terms of $|a|$ which have a_{11} as a factor is equal to

$$a_{11}\delta^{1\ 2\ \dots\ n}_{1\ \nu_2\dots\nu_n} a_{2\nu_2}\dots a_{n\nu_n}$$

$$=a_{11}\delta^{2\ \dots\ n}_{\nu_2\dots\nu_n} a_{2\nu_2}\dots a_{n\nu_n}=a_{11}M_{11} \quad \dots\dots\dots\dots\dots\dots\dots(7)$$

In the original determinant $|a|$, the p^{th} row can be brought to the top by $p-1$ successive exchanges of rows without disturbing the relative positions of the other rows, and the q^{th} column can then be brought to the left by $q-1$ exchanges without disturbing the relative positions of the other columns. The determinant so obtained is equal to $(-1)^{p-1}(-1)^{q-1}|a|$, and the first term of its top row is a_{pq} and its minor is identical with the minor of a_{pq} in $|a|$, i.e. is M_{pq}. Hence by (7) the sum of the terms of $|a|$ which have a_{pq} as a factor is equal to $(-1)^{p+q}a_{pq}M_{pq}$.

Since every term of $|a|$ involves one and only one element of the p^{th} row

$$|a| = (-1)^{p+\nu}a_{p\nu}M_{p\nu} \quad (\nu = 1 \text{ to } n) \quad \ldots\ldots\ldots\ldots\ldots\ldots (8)$$

Similarly

$$|a| = (-1)^{\mu+q}a_{\mu q}M_{\mu q} \quad (\mu = 1 \text{ to } n) \quad \ldots\ldots\ldots\ldots\ldots\ldots (9)$$

These results give the expansion of a determinant by *any* row or column. In particular, putting $p=1$,

$$|a| = (-1)^{1+\nu}a_{1\nu}M_{1\nu} \quad (\nu = 1 \text{ to } n)$$

which establishes the identity of (2) and (3) as definitions of $|a_{\mu\nu}|$.

If $(-1)^{p+q}M_{pq}$ is denoted by A_{pq}, equations (8), (9) may be written

$$|a| = a_{p\nu}A_{p\nu} \quad (\nu = 1 \text{ to } n) \quad \ldots\ldots\ldots\ldots\ldots\ldots (10)$$

$$|a| = a_{\mu q}A_{\mu q} \quad (\mu = 1 \text{ to } n) \quad \ldots\ldots\ldots\ldots\ldots\ldots (11)$$

A_{pq} is called the *co-factor* of a_{pq}.

Example 4. Evaluate $\begin{vmatrix} a & a^2 & a^4 - 1 \\ b & b^2 & b^4 - 1 \\ c & c^2 & c^4 - 1 \end{vmatrix}$

The determinant $= \begin{vmatrix} a & a^2 & a^4 \\ b & b^2 & b^4 \\ c & c^2 & c^4 \end{vmatrix} - \begin{vmatrix} a & a^2 & 1 \\ b & b^2 & 1 \\ c & c^2 & 1 \end{vmatrix} = \Delta_1 - \Delta_2$, say.

By Example 6, p. 179, $\Delta_2 = (b-c)(c-a)(a-b)(a+b+c)$; and by the same method,

$$\Delta_1/abc = (b-c)(c-a)(a-b)\{h(a^2+b^2+c^2) + k(bc+ca+ab)\}$$

where h, k are independent of a, b, c. Equating coefficients of a^4b, a^2b^2, it is found that $h=0$, $k=1$. Hence

$$\Delta_1 - \Delta_2 = (b-c)(c-a)(a-b)\{abc(bc+ca+ab) - (a+b+c)\}.$$

Example 5. Prove that

$$\begin{vmatrix} 0 & a^2 & b^2 & c^2 \\ a^2 & 0 & f^2 & e^2 \\ b^2 & f^2 & 0 & d^2 \\ c^2 & e^2 & d^2 & 0 \end{vmatrix} = \begin{vmatrix} 0 & ad & be & cf \\ ad & 0 & cf & be \\ be & cf & 0 & ad \\ cf & be & ad & 0 \end{vmatrix}$$

This is proved by multiplying the terms of the 1st, 2nd, 3rd, 4th columns of the first determinant by *def*, *bcd*, *ace*, *abf* respectively, and then dividing the rows by *abc*, *aef*, *bdf*, *cde*.

Example 6. If $X_p x_q + Y_p y_q + Z_p z_q + T_p t_q = 0$ for $p = 1, 2$ and $q = 1, 2$, and if $(\alpha\beta)$ denotes $\alpha_1\beta_2 - \alpha_2\beta_1$, prove that

$$\frac{(xt)}{(YZ)} = \frac{(yt)}{(ZX)} = \frac{(zt)}{(XY)} = \frac{(yz)}{(XT)} = \frac{(zx)}{(YT)} = \frac{(xy)}{(ZT)}$$

Elimination of T_1 from the equations given by $p = 1$, $q = 1$ and $p = 1$, $q = 2$ gives

$$X_1(xt) + Y_1(yt) + Z_1(zt) = 0$$

Similarly $$X_2(xt) + Y_2(yt) + Z_2(zt) = 0$$

Hence $$(xt) : (yt) = (YZ) : (ZX), \text{ etc.}$$

By this method all the results can be obtained. They have an important application in Geometry.

EXERCISE XVIb

A

In Nos. 1-4 give the signs of the terms of the expansions of $|a_{\mu\nu}|$.

1. $a_{13}a_{24}a_{32}a_{45}a_{51}$
2. $a_{13}a_{27}a_{36}a_{45}a_{51}a_{64}a_{72}$
3. $a_{31}a_{52}a_{13}a_{24}a_{45}$
4. $a_{32}a_{61}a_{24}a_{15}a_{43}a_{56}$

Evaluate the determinants:

5. $\begin{vmatrix} a-b & b-c & c-a \\ b-c & c-a & a-b \\ c-a & a-b & b-c \end{vmatrix}$
6. $\begin{vmatrix} 1 & bc & b+c \\ 1 & ca & c+a \\ 1 & ab & a+b \end{vmatrix}$

7. Verify that the determinants

$$\begin{vmatrix} 1 & 0 \\ x & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ x & y & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \\ x & y & 1 & 0 \\ x & y & z & 1 \end{vmatrix}, \quad \begin{vmatrix} \delta_1^1 & \delta_2^1 \\ \delta_1^2 & \delta_2^2 \end{vmatrix}$$

and $|\epsilon_{\mu\nu}|$ are all equal ($\mu, \nu = 1$ to 2).

8. Solve:

$$\begin{vmatrix} a+x & b+x & c+x \\ b+x & c+x & a+x \\ c+x & a+x & b+x \end{vmatrix} = 0$$

9. Express in factors:

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^4 & b^4 & c^4 \end{vmatrix}$$

Evaluate the determinants in Nos. 10, 11.

10. $\begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^4 & b^4 & c^4 & d^4 \end{vmatrix}$

11. $\begin{vmatrix} a & a & a & a \\ a & b & b & b \\ a & b & c & c \\ a & b & c & d \end{vmatrix}$

B

In Nos. 12-14 give the signs of the terms of the expansions of $|a_{\mu\nu}|$

12. $a_{14}a_{21}a_{32}a_{43}$ 13. $a_{51}a_{12}a_{43}a_{24}a_{35}$ 14. $a_{12}a_{61}a_{24}a_{53}a_{36}a_{45}$

15. Verify that

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & b & x \\ c & d & y \\ 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} a & b & x & z \\ c & d & y & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

Evaluate the determinants in Nos. 16, 17.

16. $\begin{vmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 2 \\ -1 & -1 & 0 & 1 \\ -1 & -2 & -1 & 0 \end{vmatrix}$

17. $\begin{vmatrix} a & b & c & d \\ a & a+b & a+b+c & a+b+c+d \\ a & 2a+b & 3a+2b+c & 4a+3b+2c+d \\ a & 3a+b & 6a+3b+c & 10a+6b+3c+d \end{vmatrix}$

18. Solve the equation $\begin{vmatrix} x & a & a & 1 \\ a & x & b & 1 \\ a & b & x & 1 \\ a & b & c & 1 \end{vmatrix} = 0$

C

19. Evaluate $\begin{vmatrix} x^3 & 1 & (x+1)^3 \\ y^3 & 1 & (y+1)^3 \\ z^3 & 1 & (z+1)^3 \end{vmatrix}$

20. Prove that $\begin{vmatrix} bcd & a & a^2 & a^3 \\ acd & b & b^2 & b^3 \\ abd & c & c^2 & c^3 \\ abc & d & d^2 & d^3 \end{vmatrix} = \begin{vmatrix} 1 & a^2 & a^3 & a^4 \\ 1 & b^2 & b^3 & b^4 \\ 1 & c^2 & c^3 & c^4 \\ 1 & d^2 & d^3 & d^4 \end{vmatrix}$

21. Prove that if $\mu_1, \mu_2, \ldots, \mu_n$ and $\nu_1, \nu_2, \ldots, \nu_n$ are permutations of 1, 2, ..., n,

$$\delta^{\mu_1\mu_2 \ldots \mu_n}_{\nu_1\nu_2 \ldots \nu_n} c_{\mu_1\nu_1} c_{\mu_2\nu_2} \ldots c_{\mu_n\nu_n} = n! \, |c|$$

22. Prove that

$$\begin{vmatrix} 1+a^2-b^2 & 2ab & -2b \\ 2ab & 1-a^2+b^2 & 2a \\ 2b & -2a & 1-a^2-b^2 \end{vmatrix} = (1+a^2+b^2)^3$$

23. If the rows of a determinant Δ are a, b, c, d, e; b, c, d, e, a; c, d, e, a, b; d, e, a, b, c; e, a, b, c, d, and if $\lambda^5 = 1$, prove that $a + \lambda b + \lambda^2 c + \lambda^3 d + \lambda^4 e$ is a factor of Δ and find all the factors.

24. Prove that the sum of the homogeneous products of degree n in a, b, c is a factor of $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^{n+2} & b^{n+2} & c^{n+2} \end{vmatrix}$

Express this determinant in factors if $n = 3$.

25. Prove that

$$\begin{vmatrix} 1+a_1 & a_2 & a_3 \ldots a_n \\ a_1 & 1+a_2 & a_3 \ldots a_n \\ \vdots & \vdots & \vdots \quad \vdots \\ a_1 & a_2 & a_3 \ldots 1+a_n \end{vmatrix} = 1 + a_1 + a_2 + \ldots + a_n$$

and deduce that

$$\begin{vmatrix} x_1 & a_1 & a_1 \ldots a_1 \\ a_2 & x_2 & a_2 \ldots a_2 \\ \vdots & \vdots & \vdots \quad \vdots \\ a_n & a_n & a_n \ldots x_n \end{vmatrix} = \left\{1 + \sum_1^n \frac{a_r}{x - a_r}\right\} \prod_1^n (x - a_r)$$

26. If $u_n = \begin{vmatrix} 1 & a & 0 & 0 & 0 & 0 \ldots \\ a & 1 & a & 0 & 0 & 0 \ldots \\ 0 & a & 1 & a & 0 & 0 \ldots \\ 0 & 0 & a & 1 & a & 0 \ldots \\ 0 & 0 & 0 & a & 1 & a \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{vmatrix}$ and the determinant is of order n, prove that $u_n = u_{n-1} - a^2 u_{n-2}$ and deduce that

$$u_n = \{(1+k)^{n+1} - (1-k)^{n+1}\}/(k 2^{n+1}) \text{ where } k = \sqrt{(1 - 4a^2)}.$$

27. If $x = 2\cos\theta$, prove that the determinant

$$\begin{vmatrix} x & 1 & 0 & 0 & 0 & 0 \dots \\ 1 & x & 1 & 0 & 0 & 0 \dots \\ 0 & 1 & x & 1 & 0 & 0 \dots \\ 0 & 0 & 1 & x & 1 & 0 \dots \\ 0 & 0 & 0 & 1 & x & 1 \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{vmatrix}$$

of order n, is equal to $\sin(n+1)\theta \operatorname{cosec}\theta$.

An important application of equation (10), page 401, is obtained by considering the new determinant formed from $|a_{\mu\nu}|$ by replacing the elements of the p^{th} row by the corresponding elements of the q^{th} row. This new determinant has two identical rows and is therefore zero. But the alteration of the p^{th} row does not affect the co-factors $A_{p\nu}$. Hence equation (10) gives

$$a_{q\nu}A_{p\nu} = 0 \qquad (\nu = 1 \text{ to } n),\ (q \neq p).$$

For $q = p$, equation (10) itself gives $a_{p\nu}A_{p\nu} = |a|$, and the results can be combined in the form

$$a_{q\nu}A_{p\nu} = \delta^p_q |a| \qquad \dots\dots\dots\dots(12)$$

Similarly
$$a_{\mu q}A_{\mu p} = \delta^p_q |a|. \qquad \dots\dots\dots\dots(13)$$

The symmetrical determinant $|a|$ of order 3 is of special importance in geometry of two dimensions and is often written as $\begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix}$ and denoted by Δ.

It follows from (12) but it is easy to verify independently that

if
$$A = bc - f^2 \qquad B = ca - g^2 \qquad C = ab - h^2$$
$$F = gh - af \qquad G = hf - bg \qquad H = fg - ch$$

then
$$\Delta = aA + hH + gG = hH + bB + fF = gG + fF + cC$$
$$0 = aH + hB + gF = hG + bF + fC = gA + fH + cG$$
$$= aG + hF + gC = hA + bH + fG = gH + fB + cF$$

Laplace's Expansion. The expansion of a determinant in the form $a_{pr}A_{pr}$ can be generalised. Consider for example

$$\Delta \equiv \begin{vmatrix} a_1 & a_2 & a_3 & p_4 & p_5 \\ b_1 & b_2 & b_3 & q_4 & q_5 \\ c_1 & c_2 & c_3 & r_4 & r_5 \\ d_1 & d_2 & d_3 & s_4 & s_5 \\ e_1 & e_2 & e_3 & t_4 & t_5 \end{vmatrix}$$

Two such determinants as $\begin{vmatrix} b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \\ e_1 & e_2 & e_3 \end{vmatrix}$, $\begin{vmatrix} p_4 & p_5 \\ s_4 & s_5 \end{vmatrix}$

are called *complementary minors* of orders 3 and 2.

If all the ten products of such complementary minors (formed one from the left and the other from the right of the dotted line) are added together after a suitable sign, + or −, has been attached to each product, the sum will be shown to be Δ. It is evident that the sum will include just those terms which are the product of elements taken one from each row and one from each column, that is it will contain just the terms of Δ. But it is necessary to show that the sign attached can be chosen so as to give all the terms of Δ with their correct signs.

Consider the general term of the determinant of order $m+n$

$$\Delta \equiv \begin{vmatrix} a_{11} & a_{12} \dots a_{1n} & b_{11} & b_{12} \dots b_{1m} \\ a_{21} & a_{22} \dots a_{2n} & b_{21} & b_{22} \dots b_{2m} \\ \vdots & \vdots \quad \vdots & \vdots & \vdots \quad \vdots \\ a_{s1} & a_{s2} \dots a_{sn} & b_{s1} & b_{s2} \dots b_{sm} \end{vmatrix}$$

where $s=m+n$ and b_{pq} has been written for $a_{p(q+n)}$

This term is $(-1)^r a_{\mu_1 1} a_{\mu_2 2} \dots a_{\mu_n n} b_{\nu_1 1} b_{\nu_2 2} \dots b_{\nu_m m}$. Here μ and ν both refer to rows. Also $(-1)^r = \epsilon_{\mu_1 \mu_2 \dots \mu_n \nu_1 \nu_2 \dots \nu_m}$ and so the value of $(-1)^r$ is found by counting the number of exchanges required to bring $\mu_1 \mu_2 \dots \mu_n \nu_1 \nu_2 \dots \nu_m$ into the order $1, 2, \dots, s$. These exchanges may be made by first bringing the μ's and ν's separately into order of magnitude in the form $\mu_1' \mu_2' \dots \mu_n' \nu_1' \nu_2' \dots \nu_m'$ and then bringing these into the order $1, 2, \dots, s$. Symbolically

$$\epsilon_{\mu_1 \dots \mu_n \nu_1 \dots \nu_m} = \delta^{\mu_1' \dots \mu_n'}_{\mu_1 \dots \mu_n} \delta^{\nu_1' \dots \nu_m'}_{\nu_1 \dots \nu_m} \epsilon_{\mu_1' \dots \mu_n' \nu_1' \dots \nu_m'}.$$

But $\delta_{\mu_1 \dots \mu_n}^{\mu_1' \dots \mu_n'} a_{\mu_1 1} \dots a_{\mu_n n}$ and $\delta_{\nu_1 \dots \nu_m}^{\nu_1' \dots \nu_m'} b_{\nu_1 1} \dots b_{\nu_m m}$ are the complementary minors and therefore if the sign of

$$\epsilon_{\mu_1' \dots \mu_n' \nu_1' \dots \nu_m'}$$

is attached to the product of these complementary minors, the sum of such products is equal to Δ; this is called a *Laplace expansion* of Δ.

In practice this sign may be found by examining the sign in Δ of the term which is the product of the leading diagonal terms of the complementary minors. In the example given above, the sign for $(b_1 c_2 e_3) \times (p_4 s_5)$ is + because the leading diagonals give $b_1 c_2 e_3 p_4 s_5$; but b, c, e, p, s come from the rows 2, 3, 5, 1, 4, and 23514 is an even permutation of 12345.

In the general determinant of order s if any particular set of r rows $\mu_1, \mu_2, \dots, \mu_r$ and any particular set of r columns $\nu_1, \nu_2, \dots, \nu_r$ are taken, the elements common to these sets (taken in the order in which they stand in Δ) form a determinant of order r which is called a *minor of order* r of Δ. The minor of order $s - r$ formed by the elements of Δ not in those r rows and columns is called the *complementary minor*.

Thus Laplace's expansion is the sum of the products, with an appropriate sign attached to each, of the minors (of order r) and their complementary minors.

In Laplace's expansion the division of Δ into two portions may not only be made between any two columns or any two rows, but by taking any selection of r columns (or rows) and the remaining $s - r$. It is usual to begin by bringing the r columns (or rows) to the left (or top). In $|a_{\mu\nu}|$, ν indicates the columns.

Assuming that $\nu_1, \nu_2, \dots, \nu_r$ are in ascending order of magnitude, these columns can be transferred to the 1st, 2nd, ..., r^{th} places in $(\nu_1 - 1) + (\nu_2 - 2) + \dots + (\nu_r - r)$ steps, without altering their relative order or the relative order of the other columns. This multiplies the value of the determinant by

$$(-1)^{(\Sigma\nu)-1-2-\dots-r}.$$

To determine the sign to be attached to any particular product in Laplace's expansion, it is convenient also to transfer the r rows $\mu_1, \mu_2, \ldots, \mu_r$ to the top. This multiplies the value of the determinant by $(-1)^{(\Sigma\mu)-1-2-\cdots-r}$. But after these transferences the sign is $+$, because the product of the leading diagonals of the complementary minors is the leading diagonal of Δ. Hence the sign required is $(-1)^{\Sigma(\mu+\nu)}$.

If then the *complementary co-factor* of the minor of order r is defined to be $(-1)^{\Sigma(\mu+\nu)}$ times the complementary minor, Laplace's expansion is the sum of the products of the minors and their complementary co-factors.

In the example given above, the values of μ for $(b_1c_2e_3)$ are 2, 3, 5, and of ν are 1, 2, 3; but $(2+3+5)+(1+2+3)$ is even, therefore the complementary co-factor of $(b_1c_2e_3)$ is $+(p_4s_4)$.

Example 7. Evaluate $\Delta \equiv \begin{vmatrix} 0 & 0 & a_1 & b_1 & c_1 \\ 0 & 0 & a_2 & b_2 & c_2 \\ x_1 & x_2 & -1 & 0 & 0 \\ y_1 & y_2 & 0 & -1 & 0 \\ z_1 & z_2 & 0 & 0 & -1 \end{vmatrix}$

First Method. Insert the Laplace dotted line after the second column, then 7 of the 10 minors formed from the first 2 columns are zero, and the remaining three products of complementary minors are

$$\begin{vmatrix} y_1 & y_2 \\ z_1 & z_2 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ -1 & 0 & 0 \end{vmatrix} \quad \begin{vmatrix} x_1 & x_2 \\ z_1 & z_2 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ 0 & -1 & 0 \end{vmatrix} \quad \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ 0 & 0 & -1 \end{vmatrix}$$

For (y_1z_2), $\Sigma\mu = 4+5$, $\Sigma\nu = 1+2$, $\Sigma(\mu+\nu) = 12$, therefore the sign is $(-1)^{12}$.

Similarly the signs for (x_1z_2), (x_1y_2) are $(-1)^{11}$, $(-1)^{10}$.

Alternatively consider the sign of the product of the leading diagonal terms.

$$\therefore \Delta = +(y_1z_2)(-1)(b_1c_2) - (x_1z_2)(a_1c_2) + (x_1y_2)(-1)(a_1b_2)$$
$$= -\Sigma\{(y_1z_2 - y_2z_1)(b_1c_2 - b_2c_1)\}.$$

Second Method. Col $1+x_1$ col $3+y_1$ col $4+z_1$ col 5,

col $2+x_2$ col $3+y_2$ col $4+z_2$ col 5,

$$\Delta=\begin{vmatrix} a_1x_1+b_1y_1+c_1z_1 & a_1x_2+b_1y_2+c_1z_2 & a_1 & b_1 & c_1 \\ a_2x_1+b_2y_1+c_2z_1 & a_2x_2+b_2y_2+c_2z_2 & a_2 & b_2 & c_2 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{vmatrix}$$

Insert the Laplace dotted line after the second column,

$$\therefore\ \Delta=\epsilon_{12345}\begin{vmatrix} a_1x_1+b_1y_1+c_1z_1 & a_1x_2+b_1y_2+c_1z_2 \\ a_2x_1+b_2y_1+c_2z_1 & a_2x_2+b_2y_2+c_2z_2 \end{vmatrix}\begin{vmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{vmatrix}$$

$$=(a_2x_1+b_2y_1+c_2z_1)(a_1x_2+b_1y_2+c_1z_2)$$
$$-(a_1x_1+b_1y_1+c_1z_1)(a_2x_2+b_2y_2+c_2z_2)$$

The equivalence of these two results is established by another method in the next chapter, see Example 4, p. 450.

An important identity which can be proved by a Laplace's expansion is given in Exercise XVIc, No. 5.

Product of two Determinants of Order n.

Let $|a|$ and $|b|$ be the two determinants.

Then $$|a|\ |b|=|a|\ \epsilon_{\mu_1\mu_2\dots\mu_n}b_{\mu_11}b_{\mu_22}\dots b_{\mu_nn}.$$

But by equation (6), page 399,

$$|a|\ \epsilon_{\mu_1\mu_2\dots\mu_n}=\epsilon_{\nu_1\nu_2\dots\nu_n}a_{\nu_1\mu_1}a_{\nu_2\mu_2}\dots a_{\nu_n\mu_n}.$$

Hence
$$|a|\ |b|=\epsilon_{\nu_1\nu_2\dots\nu_n}a_{\nu_1\mu_1}a_{\nu_2\mu_2}\dots a_{\nu_n\mu_n}b_{\mu_11}b_{\mu_22}\dots b_{\mu_nn}$$
$$=\epsilon_{\nu_1\nu_2\dots\nu_n}(a_{\nu_1\mu_1}b_{\mu_11})(a_{\nu_2\mu_2}b_{\mu_22})\dots(a_{\nu_n\mu_n}b_{\mu_nn})$$
$$=\epsilon_{\nu_1\nu_2\dots\nu_n}c_{\nu_11}c_{\nu_22}\dots c_{\nu_nn}=|c| \quad \dots\dots\dots\dots(14)$$

where c_{pq} denotes $a_{p\mu}b_{\mu q}$ ($\mu=1$ to n).

In particular if $n=2$

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}\begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix}=\begin{vmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{vmatrix}.$$

For an alternative method of proving the product formula, see Exercise XVIc, No. 8.

Other forms of the product are obtained by interchanges of rows and columns. It will be found that the standard form of product, given by $a_{p\mu}b_{\mu q}$, is the most convenient; but other forms can be obtained by replacing Δ, Δ' by their transposed determinants before multiplying.

Inner Products. The inner product of two sets of numbers $a_1, a_2, \ldots, a_n$ and $x_1, x_2, \ldots, x_n$ is the sum $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ which we denote by $a_\mu x_\mu$. It is also denoted by $a \mid x$ or by a_x.

The general element $c_{pq} \equiv a_{p\mu}b_{\mu q}$ of the determinant which is the product of $|a|$, $|b|$ and is formed by weaving the p^{th} row of $|a|$ into the q^{th} column of $|b|$ is the inner product of the p^{th} row and the q^{th} column.

Adjugate and Reciprocal Determinants. The determinant $|A|$ in which each element is the co-factor of the corresponding element of $|a|$ is called the *adjugate* of $|a|$.

Let $|B|$ be the transposed of $|A|$. Then $|B| = |A|$ and $B_{pq} = A_{qp}$. Thus the product formula on p. 409

$$|a| \times |B| = |a_{p\lambda}B_{\lambda q}|$$

gives

$$|a| \times |A| = |a_{p\lambda}A_{q\lambda}|$$

But by (12) $a_{p\lambda}A_{q\lambda}$ equals $|a|$ if $p = q$ and is zero if $p \neq q$. Hence if $|a| = \Delta$ and $|A| = \bar{\Delta}$ and n is their order

$$\Delta\bar{\Delta} = \begin{vmatrix} \Delta & 0 & 0 \ldots 0 \\ 0 & \Delta & 0 \ldots 0 \\ \vdots & \vdots & \vdots \quad \vdots \\ 0 & 0 & 0 \ldots \Delta \end{vmatrix} = \Delta^n$$

This is true for all values of $a_{\mu\nu}$; in other words it is an identity, hence (even if $\Delta = 0$)

$$\bar{\Delta} = \Delta^{n-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (15)$$

If $\Delta \neq 0$, the determinant formed by dividing every element of the adjugate of Δ by Δ is equal to $\bar{\Delta} \div \Delta^n$ and therefore Δ^{-1}. It is called the *reciprocal* determinant of Δ.

Symmetric and Skew-symmetric Determinants.

A determinant $|a_{\mu\nu}|$ is called *symmetric* if $a_{pq}=a_{qp}$ for all values of p, q and is called *skew-symmetric* if $a_{pq}=-a_{qp}$. In a skew-symmetric determinant $a_{pp}=-a_{pp}$ and therefore $a_{pp}=0$.

The adjugate of a symmetric determinant is itself symmetric.

A skew-symmetric determinant of odd order is always zero and one of even order is a perfect square function of its elements. See Exercise XVIc, Nos. 6, 7, 19. Hence it follows that the adjugate of a skew-symmetric determinant is symmetric or skew-symmetric according as its order is odd or even.

Example 8. With the notation of p. 405, prove that

$$\text{(i)}\quad \begin{vmatrix} A & H & G \\ H & B & F \\ G & F & C \end{vmatrix} \equiv \Delta^2 \qquad \text{(ii)}\ BC-F^2\equiv a\Delta \qquad \text{(iii)}\ GH-AF\equiv f\Delta$$

(i) This is a special case of (15), p. 410, when $n=3$.

(ii) From formulae (12) and (14)

$$\begin{vmatrix} 1 & 0 & 0 \\ H & B & F \\ G & F & C \end{vmatrix} \begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix} \equiv \begin{vmatrix} a & h & g \\ 0 & \Delta & 0 \\ 0 & 0 & \Delta \end{vmatrix}$$

$$\therefore\ (BC-F^2)\Delta\equiv a\Delta^2; \qquad \therefore\ BC-F^2\equiv a\Delta$$

(iii) This follows in a similar way from the identity

$$\begin{vmatrix} A & H & G \\ 0 & 0 & 1 \\ G & F & C \end{vmatrix} \begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix} \equiv \begin{vmatrix} \Delta & 0 & 0 \\ g & f & c \\ 0 & 0 & \Delta \end{vmatrix}$$

Much more general results than those of Example 8 are given for non-zero determinants by *Jacobi's Theorem* which follows.

The minors of a determinant Δ are proportional to the corresponding complementary co-factors of the reciprocal determinant Δ^{-1}.

By altering the order of appropriate rows and columns any minor of Δ can be brought to the top left corner. Therefore it is sufficient to investigate the ratio

$$(a_{11}\, a_{22} \dots a_{mm}) : (A_{m+1\,m+1} \dots A_{nn}) \div \Delta^{n-m}.$$

To illustrate the general method, consider the case $n=5$, $m=2$.

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{vmatrix} \begin{vmatrix} 1 & 0 & A_{31} & A_{41} & A_{51} \\ 0 & 1 & A_{32} & A_{42} & A_{52} \\ 0 & 0 & A_{33} & A_{43} & A_{53} \\ 0 & 0 & A_{34} & A_{44} & A_{54} \\ 0 & 0 & A_{35} & A_{45} & A_{55} \end{vmatrix} \equiv \begin{vmatrix} a_{11} & a_{12} & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 & 0 \\ a_{31} & a_{32} & \Delta & 0 & 0 \\ a_{41} & a_{42} & 0 & \Delta & 0 \\ a_{51} & a_{52} & 0 & 0 & \Delta \end{vmatrix}$$

[Note the transposition in the second determinant on the left side.]

$$\therefore\ \Delta(A_{33}A_{44}A_{55}) \equiv (a_{11}a_{22})\Delta^3$$

$$\therefore\ (A_{33}A_{44}A_{55}) \equiv (a_{11}a_{22})\Delta^2, \text{ even if } \Delta = 0.$$

In the general case Δ, $\equiv |a_{\mu\nu}|$ ($\mu, \nu = 1$ to n), is multiplied by $|B_{\nu\rho}|$ ($\nu, \rho = 1$ to n), where

$$B_{\nu\rho} \equiv \delta^{\rho}_{\nu} \text{ for } \rho \leqslant m, \quad B_{\nu\rho} \equiv A_{\rho\nu} \text{ for } \rho > m.$$

Then the product $\equiv |c_{\mu\rho}| = |a_{\mu\nu}B_{\nu\rho}|$,

and if $\rho \leqslant m$, $a_{\mu\nu}B_{\nu\rho} = a_{\mu\nu}\delta^{\rho}_{\nu} = a_{\mu\rho}$ by Example 2, p. 395,

while if $\rho > m$, $a_{\mu\nu}B_{\nu\rho} = a_{\mu\nu}A_{\rho\nu} = \delta^{\rho}_{\mu}\Delta$, by (12), p. 405.

Hence $$|c_{\mu\rho}| = (a_{11}a_{22}\dots a_{mm})\Delta^{n-m}.$$

Also $$|B_{\nu\rho}| = (A_{m+1\,m+1}\dots A_{nn}).$$

$$\therefore\ \Delta(A_{m+1\,m+1}\dots A_{nn}) \overset{c}{=} (a_{11}a_{22}\dots a_{mm})\Delta^{n-m}$$

When $\Delta \neq 0$, A_{pq}/Δ is denoted by a^{pq} so that the reciprocal determinant of $|a_{\mu\nu}|$ is $|a^{\mu\nu}|$. With this notation

$$\Delta(a^{m+1\,m+1}\dots a^{nn}) = (a_{11}a_{22}\dots a_{mm})$$

Putting $m = 1, 2, \dots, n-1$, Jacobi's Theorem may then be written

$$\frac{a_{11}}{(a^{22}\dots a^{nn})} = \frac{(a_{11}a_{22})}{(a^{33}\dots a^{nn})} = \frac{(a_{11}a_{22}a_{33})}{(a^{44}\dots a^{nn})} = \dots = \Delta$$

When $\Delta = 0$ and $n - m > 1$, it follows that $(A_{m+1\,m+1}\dots A_{nn}) = 0$ and every minor of the adjugate of order > 2 is zero.

EXERCISE XVIc

A

1. Find the signs of the following products in the Laplace's expansions of $|a_{\mu\nu}|$ (i) $(a_{21}a_{42})(a_{13}a_{24}a_{55}a_{66})$

(ii) $(a_{11}a_{22}a_{33})(a_{24}a_{65})$ (iii) $(a_{21}a_{43}a_{62})(a_{14}a_{25}a_{56})$

2. Find the complementary co-factors in $|a_{\mu\nu}|$ for

(i) $(a_{11}a_{33})$, $n=5$ (ii) $(a_{21}a_{42}a_{53})$, $n=6$ (iii) $(a_{21}a_{62}a_{65})$, $n=7$.

Use Laplace's expansions to evaluate Nos. 3, 4.

3. $\begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & c^2 & b^2 \\ 1 & c^2 & 0 & a^2 \\ 1 & b^2 & a^2 & 0 \end{vmatrix}$ 4. $\begin{vmatrix} 0 & 0 & 0 & a & b \\ 0 & 0 & e & a & b \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & d & 0 & a & 0 \\ c & 0 & 0 & 0 & b \\ c & d & e & 0 & 0 \end{vmatrix}$

5. Use the determinant whose rows are x_1, y_1, x_2, y_1 ; x_2, y_2, x_3, y_2 ; x_3, y_3, x_4, y_3 ; x_4, y_4, x_1, y_4 to prove Laplace's identity $p_{23}p_{14}+p_{31}p_{24}+p_{12}p_{34}=0$ where p_{rs} denotes $x_ry_s-x_sy_r$.

6. Verify that $\begin{vmatrix} 0 & a \\ -a & 0 \end{vmatrix}$ and $\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix}$ are perfect squares.

7. (i) Verify that the skew-symmetric determinant $\begin{vmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{vmatrix}$ is zero by changing the signs of all its elements. Also find the adjugate determinant.

(ii) Prove that any skew-symmetric determinant of odd order is zero.

8. Prove the formula for the product of two determinants of order 3 by applying the transformations, col $4+\sum_1^3 b_{r1}$ col r, col $5+\sum_1^3 b_{r2}$ col r, col $6+\sum_1^3 b_{r3}$ col r to the determinant

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & 0 & 0 & 0 \\ a_{21} & a_{22} & a_{23} & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 & 0 \\ -1 & 0 & 0 & b_{11} & b_{12} & b_{13} \\ 0 & -1 & 0 & b_{21} & b_{22} & b_{23} \\ 0 & 0 & -1 & b_{31} & b_{32} & b_{33} \end{vmatrix}$$

9. If $ax+by+cz=1$, $cx+ay+bz=0$, $bx+cy+az=0$, prove that $\begin{vmatrix} x & y & z \\ z & x & y \\ y & z & x \end{vmatrix}$ and $\begin{vmatrix} a & c & b \\ b & a & c \\ c & b & a \end{vmatrix}$ have reciprocal values and

$$\begin{vmatrix} ax+cy+bz & bx+ay+cz & cx+by+az \\ by+az+cx & cy+bz+ax & ay+cz+bx \\ cz+bx+ay & az+cx+by & bz+ax+cy \end{vmatrix} = 1$$

10. Obtain the necessary condition for

$$ax^2+by^2+cz^2+2fyz+2gzx+2hxy$$

to be the product of linear factors $l_1x+m_1y+n_1z$, $l_2x+m_2y+n_2z$ by forming the product

$$\begin{vmatrix} l_1 & l_2 & 0 \\ m_1 & m_2 & 0 \\ n_1 & n_2 & 0 \end{vmatrix} \begin{vmatrix} l_2 & m_2 & n_2 \\ l_1 & m_1 & n_1 \\ 0 & 0 & 0 \end{vmatrix}$$

11. Show that the reciprocal of the reciprocal of a determinant Δ is identical with Δ, element for element.

B

12. Find the sign of the product $(a_{22}\,a_{43})(a_{11}\,a_{24}\,a_{55}\,a_{66})$ in Laplace's expansion of $|a_{\mu\nu}|$

13. Find the complementary co-factor of $(a_{23}\,a_{35}\,a_{56}\,a_{77})$ in the determinant $|a_{\mu\nu}|$ of order 7.

Use Laplace's expansions to evaluate :

14. $\begin{vmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{vmatrix}$ **15.** $\begin{vmatrix} a & h & g & x_1 & x_2 \\ h & b & f & y_1 & y_2 \\ g & f & c & z_1 & z_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_1 & y_1 & z_1 & 0 & 0 \\ x_2 & y_2 & z_2 & 0 & 0 \end{vmatrix}$

16. Evaluate $\begin{vmatrix} a+bi & c+di \\ -c+di & a-bi \end{vmatrix} \begin{vmatrix} p-qi & -r-si \\ r-si & p+qi \end{vmatrix}$

and hence express $(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)$ as the sum of four squares.

17. If $x=a^2+2bc$, $y=b^2+2ca$, $z=c^2+2ab$, $s=a^2+b^2+c^2$, $p=bc+ca+ab$, prove that

$$\begin{vmatrix} a & b & c \\ c & a & b \\ b & c & a \end{vmatrix}^2 = \begin{vmatrix} x & z & y \\ y & x & z \\ z & y & x \end{vmatrix} = \begin{vmatrix} s & p & p \\ p & s & p \\ p & p & s \end{vmatrix}$$

$$= \begin{vmatrix} 2bc-a^2 & c^2 & b^2 \\ c^2 & 2ca-b^2 & a^2 \\ b^2 & a^2 & 2ab-c^2 \end{vmatrix}$$

18. Express $\begin{vmatrix} b^2+c^2 & ab & ac \\ ba & c^2+a^2 & bc \\ ca & cb & a^2+b^2 \end{vmatrix}$ as the square of a determinant and hence write down its value.

C

19. (i) Prove that the adjugate of a skew-symmetric determinant of even order is skew-symmetric.

(ii) If $\Delta \equiv |a_{\mu\nu}|$ $(\mu, \nu = 1 \text{ to } 4)$ and Δ is skew-symmetric, prove that Δ is the square of a rational function of its elements by showing that $\Delta a_{12}^{\ 2} = A_{34}^{\ 2}$. See p. 411.

(iii) If $\Delta \equiv |a_{\mu\nu}|$ $(\mu, \nu = 1 \text{ to } 6)$ and Δ is skew-symmetric, prove that $\Delta^3 a_{56}^{\ 2} = (A_{11} A_{22} A_{33} A_{44})$ and deduce that Δ is the square of a rational function of its elements.

20. If the three distinct lines $ax \sec\phi - by \operatorname{cosec}\phi = c^2$ given by $\phi = \phi_1, \phi_2, \phi_3$ are concurrent, prove that

$$\sin(\phi_2 + \phi_3) + \sin(\phi_3 + \phi_1) + \sin(\phi_1 + \phi_2) = 0$$

by using the product

$$\begin{vmatrix} \sin\phi_1 & \cos\phi_1 & \sin 2\phi_1 \\ \sin\phi_2 & \cos\phi_2 & \sin 2\phi_2 \\ \sin\phi_3 & \cos\phi_3 & \sin 2\phi_3 \end{vmatrix} \begin{vmatrix} \sum\cos\phi - \cos\sum\phi & 0 & 1 \\ \sum\sin\phi + \sin\sum\phi & 1 & 0 \\ -1 & 0 & 0 \end{vmatrix}$$

21. If $\Delta = (a_1\, b_2\, c_3\, d_4)$ and if with the notation of p. 412, Δ^{-1} is denoted by $(a^1\, b^2\, c^3\, d^4)$, prove that with the notation of p. 410,

(i) $$\Delta \begin{vmatrix} x_1 & b^1 & c^1 & d^1 \\ x_2 & b^2 & c^2 & d^2 \\ x_3 & b^3 & c^3 & d^3 \\ x_4 & b^4 & c^4 & d^4 \end{vmatrix} = a_x$$

(ii) $$\Delta \begin{vmatrix} x_1 & y_1 & c^1 & d^1 \\ x_2 & y_2 & c^2 & d^2 \\ x_3 & y_3 & c^3 & d^3 \\ x_4 & y_4 & c^4 & d^4 \end{vmatrix} = \begin{vmatrix} a_x & b_x \\ a_y & b_y \end{vmatrix}$$

Deduce that $$\Sigma \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \begin{vmatrix} a_x & b_x \\ a_y & b_y \end{vmatrix}$$

22. Prove that $$\begin{vmatrix} 1 & a & x & ax \\ 1 & b & y & by \\ 1 & c & z & cz \\ 1 & d & t & dt \end{vmatrix} = \begin{vmatrix} 1 & bc+ad & yz+xt \\ 1 & ca+bd & zx+yt \\ 1 & ab+cd & xy+zt \end{vmatrix}$$

23. Express as a determinant

$$\begin{vmatrix} 2bc-a^2 & a^2 & a^2 \\ b^2 & 2ca-b^2 & b^2 \\ c^2 & c^2 & 2ab-c^2 \end{vmatrix} \div \begin{vmatrix} -a & a & a \\ c & c & -c \\ b & -b & b \end{vmatrix}$$

24. Prove that

$$\begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & a^2+\alpha^2 & ab+\alpha\beta & ac+\alpha\gamma \\ 1 & ab+\alpha\beta & b^2+\beta^2 & bc+\beta\gamma \\ 1 & ac+\alpha\gamma & bc+\beta\gamma & c^2+\gamma^2 \end{vmatrix} = -\begin{vmatrix} 1 & a & \alpha \\ 1 & b & \beta \\ 1 & c & \gamma \end{vmatrix}^2$$

25. If $s_k = \alpha^k + \beta^k + \gamma^k$, express as a determinant

$$\begin{vmatrix} s_6 & s_5 & s_4 & s_3 & x^3 \\ s_5 & s_4 & s_3 & s_2 & x^2 \\ s_4 & s_3 & s_2 & s_1 & x \\ s_3 & s_2 & s_1 & s_0 & 1 \\ y^3 & y^2 & y & 1 & 0 \end{vmatrix} \div \begin{vmatrix} \alpha^3 & \beta^3 & \gamma^3 & x^3 & 0 \\ \alpha^2 & \beta^2 & \gamma^2 & x^2 & 0 \\ \alpha & \beta & \gamma & x & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

and hence factorise the first determinant.

26. What identity is found by applying the method of No. 5 to the determinant of order 6 with rows $x_p, y_p, z_p, x_p, y_p, z_p$ $(p = 1 \text{ to } 6)$?

27. Verify that

$$\begin{vmatrix} a_1 & b_1 & c_1 & d_1 & 0 & 0 \\ a_2 & b_2 & c_2 & d_2 & 0 & 0 \\ a_3 & b_3 & c_3 & d_3 & 0 & 0 \\ 0 & 0 & 0 & d_1 & e_1 & f_1 \\ 0 & 0 & 0 & d_2 & e_2 & f_2 \\ 0 & 0 & 0 & d_3 & e_3 & f_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 & d_1 & 0 & 0 \\ a_2 & b_2 & c_2 & d_2 & 0 & 0 \\ a_3 & b_3 & c_3 & d_3 & 0 & 0 \\ -a_1 & -b_1 & -c_1 & 0 & e_1 & f_1 \\ -a_2 & -b_2 & -c_2 & 0 & e_2 & f_2 \\ -a_3 & -b_3 & -c_3 & 0 & e_3 & f_3 \end{vmatrix}$$

and deduce the identity

$$(abc)(def) = (bcd)(aef) - (acd)(bef) + (abd)(cef)$$

where (xyz) denotes the determinant $(x_1\, y_2\, z_3)$.

MISCELLANEOUS EXAMPLES

EXERCISE XVId

A

Factorise the determinants in Nos. 1, 2.

1. $\begin{vmatrix} a^2 & ax & x^2 \\ b^2 & by & y^2 \\ c^2 & cz & z^2 \end{vmatrix}$

2. $\begin{vmatrix} 1 & a & a^2 & 0 \\ 0 & 1 & a & a^2 \\ a^2 & 0 & 1 & a \\ a & a^2 & 0 & 1 \end{vmatrix}$

3. If the equations $x^3+px^2+qx+r=0$, $x^2+ax+b=0$ have a common root, prove that $\begin{vmatrix} 1 & 0 & 1 & a-p \\ a & 1 & p & b-q \\ b & a & q & -r \\ 0 & b & r & 0 \end{vmatrix}=0$

4. Prove that

$$\begin{vmatrix} a^2+x^2 & ab-cx & ac+bx \\ ab+cx & b^2+x^2 & bc-ax \\ ac-bx & bc+ax & c^2+x^2 \end{vmatrix} = \begin{vmatrix} x & c & -b \\ -c & x & a \\ b & -a & x \end{vmatrix}^2$$

5. Find the square roots of $\begin{vmatrix} yz-x^2 & zx-y^2 & xy-z^2 \\ zx-y^2 & xy-z^2 & yz-x^2 \\ xy-z^2 & yz-x^2 & zx-y^2 \end{vmatrix}$

6. If a_{pq} is x or y according as p is or is not equal to q, prove that $|a_{\mu\nu}|=(x-y)^{n-1}\{x+(n-1)y\}$ $(\mu, \nu=1 \text{ to } n)$.

7. Evaluate $\begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^{n+3} & b^{n+3} & c^{n+3} & d^{n+3} \end{vmatrix} \div \begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{vmatrix}$

8. If $f(z)=\begin{vmatrix} a+z & h & g \\ h & b+z & f \\ g & f & c+z \end{vmatrix}$, prove that with the notation of p. 405,

$$f(z)f(-z)=\Delta^2-z^2\Sigma(A^2+2F^2)+z^4\Sigma(a^2+2f^2)-z^6,$$

and deduce that $f(z)=0$ cannot have a y-axal root. Hence prove that it has three x-axal roots.

9. If $a_{pq}=1$ for $p=q-1$, q or $q+1$, and is otherwise zero, and $|a_{\mu\nu}|$ is of order n and is denoted by D_n, prove that

$$D_{6m}=D_{6m+1}=1,\ D_{6m+2}=D_{6m+5}=0,\ \text{and}\ D_{6m+3}=D_{6m+4}=-1,$$

where m is a positive integer.

B

Evaluate the determinants in Nos. 10, 11.

10. $\begin{vmatrix} a & b & 0 & 0 \\ 0 & 0 & c & d \\ d & -c & -b & a \\ c & d & a & b \end{vmatrix}$ 11. $\begin{vmatrix} a & -b & c & -d \\ b & a & d & c \\ -c & -d & a & b \\ d & -c & -b & a \end{vmatrix}$

12. Express $|a_{\lambda\mu}|\,|b_{\nu\rho}|$ ($\lambda, \mu = 1, 2$; $\nu, \rho = 1$ to 4) as a determinant of order 4

13. If $A_p a_q + B_p b_q + C_p c_q + D_p d_q = 0$ for $p = 1, 2$ and $q = 1, 2$, and $(\alpha\beta)$ denotes $\alpha_1\beta_2 - \alpha_2\beta_1$, prove that

$$(BC) : (ad) = (AD) : (bc).$$

14. Evaluate $\begin{vmatrix} 0 & a & b & c & d \\ -a & 0 & e & 0 & c \\ -b & -e & 0 & -e & b \\ -c & 0 & e & 0 & -a \\ d & -c & -b & a & 0 \end{vmatrix}$

15. If the equations

$$a_1x^3 + b_1x^2 + c_1x + d_1 = 0, \quad a_2x^3 + b_2x^2 + c_2x + d_2 = 0$$

have a common root and (yz) denotes $y_1z_2 - y_2z_1$, prove that

$$\begin{vmatrix} (ab) & (ac) & (ad) \\ (ac) & (ad) + (bc) & (bd) \\ (ad) & (bd) & (cd) \end{vmatrix} = 0$$

C

16. If $s = \alpha + \beta + \gamma$, $q = \beta\gamma + \gamma\alpha + \alpha\beta$, $p = \alpha\beta\gamma$, prove that

$$\begin{vmatrix} 1 & -s & q & -p \\ -p & 1 & -s & q \\ q & -p & 1 & -s \\ -s & q & -p & 1 \end{vmatrix} = (1-\alpha^4)(1-\beta^4)(1-\gamma^4)$$

17. Evaluate by means of the determinants in No. 4:

$$\begin{vmatrix} x^2+a^2-b^2-c^2 & 2(ab-cx) & 2(ac+bx) \\ 2(ab+cx) & x^2+b^2-c^2-a^2 & 2(bc-ax) \\ 2(ac-bx) & 2(bc+ax) & x^2+c^2-a^2-b^2 \end{vmatrix}$$

18. If $D_n = |a_{\mu\nu}|$ $(\mu, \nu = 1 \text{ to } n)$ and $a_{pq} = u_{n-p} - x$ for $p = q$, $a_{pq} = -u_{n-q}x$ for $p = q+1$, $a_{pq} = 1$ for $p = q-1$, and otherwise $a_{pq} = 0$, prove that $D_{n+1} + xD_n = u_0 u_1 \dots u_n$, and find D_n.

19. If $a_1, a_2, \dots, a_n$ are in A.P. with common difference b, prove that the value of the determinant whose r^{th} row is $a_r, a_{r+1}, \dots, a_n, a_1, a_2, \dots, a_{r-1}$ is $(nb)^{n-1}\{a_1 + \frac{1}{2}(n-1)b\}(-1)^{n(n-1)/2}$.

20. If the equation $f(z) = 0$ of No. 8 has a double root $z = \alpha$, prove that $z - \alpha$ is a factor of each minor of the determinant. Hence with the notation of p. 405, prove that $F : G : H = f : g : h$.

21. If $a_{pq} = \dfrac{(n+p-1)!}{(q-1)!(n+p-q)!}$ $(p, q = 1 \text{ to } n)$, prove that $|a_{pq}| = 1$.

22. If $a_{pq} = a$ for $p = q$, $a_{pq} = 1$ for $p = q-1$, $a_{pq} = -1$ for $p = q+1$, and otherwise $a_{pq} = 0$, and if $|a_{\mu\nu}|$ is of order n and is denoted by D_n, prove that $D_n = aD_{n-1} + D_{n-2}$ and deduce that

$$D_n = \{[a + \sqrt{(a^2+4)}]^{n+1} - [a - \sqrt{(a^2+4)}]^{n+1}\}/\{2^{n+1}\sqrt{(a^2+4)}\}$$

23. If $a(x) = a_0x^3 + a_1x^2 + a_2x + a_3 \equiv (x - \lambda)(p_0x^2 + p_1x + p_2)$,

$$b(x) = b_0x^3 + b_1x^2 + b_2x + b_3 \equiv (x - \lambda)(q_0x^2 + q_1x + q_2),$$

prove that
$$\Delta \equiv \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 \\ 0 & 0 & b_0 & b_1 & b_2 & b_3 \\ 0 & b_0 & b_1 & b_2 & b_3 & 0 \\ b_0 & b_1 & b_2 & b_3 & 0 & 0 \end{vmatrix} = 0$$

and if Δ_1 is the determinant of order 4 formed from Δ by striking out the first and last rows and columns, prove that

$$\Delta_1 \begin{vmatrix} 1 & \lambda & \lambda^2 & \lambda^3 \\ 0 & 1 & \lambda & \lambda^2 \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} p_0 & p_1 & p_2 & 0 \\ 0 & p_0 & p_1 & p_2 \\ 0 & q_0 & q_1 & q_2 \\ q_0 & q_1 & q_2 & 0 \end{vmatrix}$$

and that the equations $a(x) = 0$, $b(x) = 0$ have two roots in common if $\Delta = 0$ and $\Delta_1 = 0$.

CHAPTER XVII

MATRICES

Linear Equations. In the solution of m linear equations

$$a_{1r}x_r + b_1 \equiv a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1 = 0$$
$$a_{2r}x_r + b_2 \equiv a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n + b_2 = 0$$
$$\ldots \qquad \ldots \qquad \ldots$$
$$a_{mr}x_r + b_m \equiv a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n + b_n = 0$$

for n variables, there are three possibilities :

(i) *no* solution, i.e. the equations are inconsistent,

(ii) a *unique* solution,

(iii) *more than one* solution.

For example in the geometry of a plane, the equations

$$a_\lambda x + b_\lambda y + c_\lambda = 0 \qquad (\lambda = 1 \text{ to } 3)$$

represent three straight lines, and the following cases occur.

(i) (*a*) the lines meet in pairs in three distinct points,

(*b*) two lines are parallel and the third meets them,

(*c*) the three lines are parallel,

(*d*) two lines are coincident and the third is parallel to them,

(ii) (*a*) the lines are distinct and meet in a point,

(*b*) two lines are coincident and the third meets them,

(iii) the three lines are coincident.

In (i) there is *no* common point, in (ii) there is *one*, and in (iii) there is an *infinity* of common points.

(i) *a* and (i) *b* are essentially different from the other cases and would be different even in the homogeneous geometry of lines $a_\lambda x + b_\lambda y + c_\lambda z = 0$. Except in these two cases, numbers k_1, k_2, k_3 not all zero, exist such that

$$k_1a_1 + k_2a_2 + k_3a_3 = 0 \quad k_1b_1 + k_2b_2 + k_3b_3 = 0 \quad k_1c_1 + k_2c_2 + k_3c_3 = 0$$

and therefore the first step in the discrimination between the seven cases turns on the dependence or independence of the sets a_1, b_1, c_1; a_2, b_2, c_2; a_3, b_3, c_3. Further steps will also be found to turn on properties of the array of coefficients. It is therefore convenient to begin with certain considerations about arrays of numbers and dependence of sets.

Matrices. A rectangular array of numbers (elements) containing m rows and n columns is called a *matrix*. The elements are enclosed in square brackets thus:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix}$$

and this matrix may be denoted by $[a_{\mu\nu}]$ or $[a]$ or by A. It may be called an $m \times n$ matrix. Some writers use round instead of square brackets.

In any element $a_{\mu\omega}$ the first suffix indicates the row and the second suffix indicates the column in which the element $a_{\mu\omega}$ occurs.

Various determinants of orders not exceeding m or n are regarded as contained in the matrix, but no numerical value is assigned to the matrix itself. If $m = n$, the determinant $|a_{\mu\nu}|$ is called *the* determinant of the matrix and may be denoted by $|\mathsf{A}|$.

Conformable matrices are those which have the same value of m and also the same value of n. Two matrices are called *equal* only when they are conformable and have their corresponding elements equal.

The cartesian coordinates of a point in three dimensions or the homogeneous coordinates of a point in two dimensions may be regarded as forming a *row-matrix* $[x\ y\ z]$ and the coordinates of a line in three dimensions are given by the six second-order determinants contained in either of the matrices

$$\begin{bmatrix} l & m & n & 0 \\ \alpha & \beta & \gamma & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} x_1 & y_1 & z_1 & t_1 \\ x_2 & y_2 & z_2 & t_2 \end{bmatrix}.$$

The matrix whose rows are identical with the columns of $[a_{\mu\nu}]$ is called the *transposed* matrix of $[a_{\mu\nu}]$. Its columns are identical with the rows of $[a_{\mu\nu}]$. The transposed matrix of A is denoted by A' and thus the *column-matrix* $\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ obtained by transposing the row-matrix $[x_1\ x_2 \dots x_n]$ is denoted by $[x_1\ x_2 \dots x_n]'$. Alternatively it is sometimes denoted by $\{x_1\ x_2 \dots x_n\}$.

Rank of a Matrix. In applications of matrices to linear equations an important idea is that of the *rank* of the matrix. A matrix is said to be of rank r when it contains at least one non-zero determinant of order r and no such determinant of order $r+1$. The rank of a matrix A may be denoted by $r(A)$.

Evidently $r \leqslant m$ and $r \leqslant n$. Also if the matrix contains a non-zero determinant of order s, it must contain at least one non-zero determinant of every order less than s.

The interdependence of the rows of a matrix is connected with the rank.

Linear Dependence. The m sets $a_{11}, a_{12}, \dots, a_{1n}$; $a_{21}, a_{22}, \dots, a_{2n}$; .....; $a_{m1}, a_{m2}, \dots, a_{mn}$; of n numbers each (not all zero in any one set) are said to be *linearly dependent* if there exist m constants $\kappa_1, \kappa_2, \dots, \kappa_m$, *not all zero*, such that

$$\kappa_1 a_{11} + \kappa_2 a_{21} + \dots + \kappa_m a_{m1} = 0$$
$$\kappa_1 a_{12} + \kappa_2 a_{22} + \dots + \kappa_m a_{m2} = 0$$
$$\dots\dots\dots\dots\dots$$
$$\kappa_1 a_{1n} + \kappa_2 a_{2n} + \dots + \kappa_m a_{mn} = 0$$

and if no such constants exist the sets are said to be *independent*.

Since *some* of the constants κ may be zero, it is not always possible to express *each* of the dependent sets linearly in terms of the others, but it is always possible to express *one* of them in this way. For example, the sets 1, 1, 1; 1, 3, 5; 12, 32, 52; 1, 4, 8, are linearly dependent ($\kappa_1 = 2$, $\kappa_2 = 10$, $\kappa_3 = -1$, $\kappa_4 = 0$)

and any of the first three can be expressed in terms of the others; but 1, 4, 8 cannot be expressed in terms of the first three.

When sets are linearly dependent, a set which can be expressed in terms of the others is said to be dependent on the others; it must be possible to choose the κ corresponding to such a set so that it is not zero.

If some of the m sets form a linearly dependent sub-set, then the m sets themselves are linearly dependent.

Dependence of the Rows or Columns of a Matrix.

If the rank of a matrix of m rows and n columns is r, the rows are linearly independent only if $r = m < n$; otherwise there are r rows on which the remaining $m - r$ rows depend.

Similarly the columns are linearly independent only if $r = n < m$; otherwise there are r columns on which the remaining columns depend.

These general statements may be proved by the same methods as are used for the following special examples which represent all the possible cases, namely

(i) $r < m$ and $r < n$

(ii) $r = n < m$

(iii) $r = m < n$.

(i) Suppose that the matrix $\begin{bmatrix} a_{11} & a_{12} & a_{13} \dots a_{18} \\ a_{21} & a_{22} & a_{23} \dots a_{28} \\ \vdots & \vdots & \vdots \quad \vdots \\ a_{61} & a_{62} & a_{63} \dots a_{68} \end{bmatrix}$

for which $m = 6$, $n = 8$, is of rank 3. Thus $r < m < n$.

Then $[a_{\mu\omega}]$ contains at least one determinant of order 3 which is not zero. Let this be $(a_{11}\ a_{22}\ a_{33})$.

The determinant $\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{1q} \\ a_{21} & a_{22} & a_{23} & a_{2q} \\ a_{31} & a_{32} & a_{33} & a_{3q} \\ a_{p1} & a_{p2} & a_{p3} & a_{pq} \end{vmatrix}$ in which p has any

of the values 4, 5, 6, is zero for $q = 1, 2, 3$, because two columns are identical, and is also zero for any value of q from 4 to 8 because the matrix is of rank 3.

Regard p as fixed and denote the co-factors of a_{1q}, a_{2q}, a_{3q}, a_{pq} by A_{1q}, A_{2q}, A_{3q}, A_{pq}. These co-factors are independent of q, and they are not all zero because $A_{pq}=(a_{11}\ a_{22}\ a_{33})$. Hence the relation

$$A_{1q}a_{1q}+A_{2q}a_{2q}+A_{3q}a_{3q}+A_{pq}a_{pq}=0$$

which holds for $q=1, 2, \ldots, 8$, shows that the p^{th} row is dependent on the first 3 rows; and p may be 4, 5, or 6.

The argument just used may be applied also when $r<n\leqslant m$. For example if $m=13$, $n=8$, $r=3$, p would be any of the numbers 4, 5, ..., 13.

(ii) Suppose that the matrix $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \vdots & \vdots & \vdots \\ a_{71} & a_{72} & a_{73} \end{bmatrix}$

for which $m=7$, $n=3$, is of rank 3. Thus $r=n<m$.

Then $[a_{\mu\nu}]$ contains at least one determinant of order 3 which is not zero. Let this be $(a_{11}\ a_{22}\ a_{33})$.

The determinant $\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{1q} \\ a_{21} & a_{22} & a_{23} & a_{2q} \\ a_{31} & a_{32} & a_{33} & a_{3q} \\ a_{p1} & a_{p2} & a_{p3} & a_{pq} \end{vmatrix}$ in which p has any

of the values 4 to 7, is zero for $q=1, 2, 3$ because two columns are identical. The co-factors A_{1q}, A_{2q}, A_{3q}, A_{pq} are not all zero because $A_{pq}=(a_{11}\ a_{22}\ a_{33})$, and they are the same for $q=1, 2, 3$. Hence

$$A_{1q}a_{1\nu}+A_{2q}a_{2\nu}+A_{3q}a_{3\nu}+A_{pq}a_{p\nu}=0 \qquad (\nu=1, 2, 3)$$

where p has any of the values 4 to 7. This shows that each of the last 4 rows of $[a_{\mu\nu}]$ is dependent on the first 3 rows.

(iii) Suppose that the matrix $\begin{bmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1r} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2r} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s1} & a_{s2} & a_{s3} & \ldots & a_{sr} \end{bmatrix}$

for which $m=5$, $n=7$, is of rank 5. Thus $r=m<n$.

Then if constants $\kappa_1, \kappa_2, \ldots, \kappa_5$ exist, not all zero, such that

$$\kappa_1 a_{1q}+\kappa_2 a_{2q}+\ldots+\kappa_5 a_{5q}=0 \qquad (q=1 \text{ to } 7)$$

every determinant of order 5 in the matrix is zero; but this is impossible because the rank is 5. Therefore the rows are independent.

The argument just used may be applied also when $r=m=n$.

It follows from (i) (ii) (iii) that the rows are linearly independent only when $r=m\leqslant n$.

Similar arguments may be used for columns.

Dependence of Linear Forms.

When the m sets $a_{\mu 1}, a_{\mu 2}, \ldots, a_{\mu n}$ $(\mu=1 \text{ to } m)$ of n numbers each are linearly dependent, the m functions

$$f_\mu \equiv a_{\mu\nu}x_\nu \qquad (\nu=1 \text{ to } n)$$

of the variables x_ν are said to be linearly dependent because the n equations

$$\kappa_1 a_{1q}+\kappa_2 a_{2q}+\ldots+\kappa_m a_{mq}=0 \qquad (q=1 \text{ to } n)$$

imply the identity

$$\kappa_1 f_1+\kappa_2 f_2+\ldots+\kappa_m f_m\equiv 0$$

Thus it follows from what has been proved about the rows of a matrix that $f_1, f_2, \ldots, f_m$ are only independent if the rank r of the matrix of their coefficients satisfies $r=m\leqslant n$.

n Linear Equations for n Variables.

$$\left.\begin{aligned} f_1 &\equiv a_{1\nu}x_\nu+b_1=0\\ f_2 &\equiv a_{2\nu}x_\nu+b_2=0\\ &\cdots\cdots\cdots\\ f_n &\equiv a_{n\nu}x_\nu+b_n=0 \end{aligned}\right\} \quad \nu=1 \text{ to } n.$$

The possible results (see p. 420) can be conveniently stated in terms of the ranks δ and ϵ of the matrices

$$\mathsf{D}\equiv\begin{bmatrix} a_{11} & a_{12}\ldots a_{1n}\\ a_{21} & a_{22}\ldots a_{2n}\\ \vdots & \\ a_{n1} & a_{n2}\ldots a_{nn}\end{bmatrix} \quad \text{and} \quad \mathsf{E}\equiv\begin{bmatrix} a_{11} & a_{12}\ldots a_{1n} & b_1\\ a_{21} & a_{22}\ldots a_{2n} & b_2\\ \vdots & & \\ a_{n1} & a_{n2}\ldots a_{nn} & b_n\end{bmatrix}.$$

The determinants contained in D are also contained in E; therefore $\epsilon\geqslant\delta$. Also if the coefficients of $x_1, x_2, \ldots, x_n$ are not all to vanish, $\delta\geqslant 1$.

For $n=2$ the reader should prove the following statements and interpret them in terms of the coordinates (x_1, x_2) of a point in a plane.

(i) If $\delta=2$ (and therefore $\epsilon=2$), the equations have the unique solution $x_1 : -x_2 : 1 = (a_{12}\ b_2) : (a_{11}\ b_2) : (a_{11}\ a_{22})$.

(ii) If $\delta=\epsilon=1$, the equations are identical and have an unlimited number (∞) of solutions. The value of one variable can be assigned at random and the value of the other is then uniquely determined.

(iii) If $\delta=1$, $\epsilon=2$, the equations are inconsistent.

For $n=3$ the equations may be taken as representing three planes in geometry of three dimensions.

(i) If $\delta=3$ (and therefore $\epsilon=3$), there is *a unique solution* (see p. 181):

$$x_1 : -x_2 : x_3 : -1$$
$$= (a_{12}\ a_{23}\ b_3) : (a_{11}\ a_{33}\ b_3) : (a_{11}\ a_{22}\ b_2) : (a_{11}\ a_{23}\ a_{33}).$$

(ii) If $\delta=\epsilon<3$, there is *an infinity of solutions.*

(*a*) Let $\delta=\epsilon=2$. Then for $\mu=1$, 2, or 3

$$A_{1\mu}f_1 + A_{2\mu}f_2 + A_{3\mu}f_3 \equiv A_{\rho\mu}f_\rho \qquad (\rho=1 \text{ to } 3)$$

where $A_{\mu\nu}$ is the co-factor of $a_{\mu\nu}$ in $|a|$. And

$$A_{\rho\mu}f_\rho = A_{\rho\mu}(a_{\rho\nu}x_\nu + b_\rho) = (a_{\rho\nu}A_{\rho\mu})x_\nu + (b_\rho A_{\rho\mu})$$

Since $\delta<3$, $|a|=0$, and hence $a_{\rho\nu}A_{\rho\mu}=0$ by p. 405.
Also, since $\epsilon<3$, $b_\rho A_{\rho\mu}=0$.

$$\therefore\ A_{1\mu}f_1 + A_{2\mu}f_2 + A_{3\mu}f_3 = 0 \qquad (\mu=1 \text{ to } 3).$$

Since $\delta>1$, the nine numbers $A_{\rho\mu}$ are not all zero and therefore f_1, f_2, f_3 are linearly dependent.

Thus there is at least one variable whose value can be assigned at random. The others are uniquely determined by two of the equations since one at least of the A's is not zero. The equations are said to have ∞ solutions.

(*b*) Let $\delta = \epsilon = 1$. Then every second order determinant of E is zero. Hence

$$a_{11} : a_{12} : a_{13} : b_1 = a_{21} : a_{22} : a_{23} : b_2 = a_{31} : a_{32} : a_{33} : b_3$$

so that the equations are identical. They are said to have ∞^2 solutions : arbitrary values can be assigned to two of the variables and the other is then uniquely determined by one of the equations.

(iii) If $\delta \neq \epsilon$, the equations are *inconsistent*.

(*a*) Let $\delta = 2$, $\epsilon = 3$. Then as in (ii *a*)

$$A_{1\mu}f_1 + A_{2\mu}f_2 + A_{3\mu}f_3 = (a_{\rho\nu}A_{\rho\mu})x_\nu + (b_\rho A_{\rho\mu}) \qquad (\rho = 1 \text{ to } 3)$$

and $a_{\rho\nu}A_{\rho\mu} = 0$.

But since $\epsilon = 3$, there is at least one value of μ for which $b_\rho A_{\rho\mu} \neq 0$. Hence for this value of μ

$$A_{1\mu}f_1 + A_{2\mu}f_2 + A_{3\mu}f_3 \neq 0$$

and this implies that no values of the variables exist such that $f_1 = 0, f_2 = 0, f_3 = 0$.

(*b*) Let $\delta = 1$, $\epsilon = 2$. Then there is one determinant $\begin{vmatrix} a_{pr} & b_p \\ a_{qr} & b_q \end{vmatrix}$ that is not zero, and in it either a_{pr} or a_{qr} is not zero. Also because $\delta = 1$

$$\begin{vmatrix} a_{pr} & f_p \\ a_{qr} & f_q \end{vmatrix} \equiv \begin{vmatrix} a_{pr} & b_p \\ a_{qr} & b_q \end{vmatrix} \neq 0$$

Hence no values of the variables exist such that $f_p = 0, f_q = 0$.

(*c*) $\delta = 1$, $\epsilon = 3$ is impossible because $\delta = 1$ implies that all the third-order determinants of E are zero.

The geometrical interpretations of these results are as follows.

In (i), the three planes have a unique common point.

In (ii *a*), they have a common line and are called collinear ; it may happen that two coincide and the third meets them.

In (ii *b*), the three planes are coincident.

In (iii *a*), one plane is parallel to the line of intersection of the others ; it may be parallel to one of them.

In (iii *b*), the three planes are parallel and at least two of them are distinct.

In the general case the equations may be written

$$f_\mu \equiv a_{\mu\nu}x_\nu + b_\mu = 0 \qquad (\mu = 1 \text{ to } n,\ \nu = 1 \text{ to } n).$$

(i) If $\delta = n$ (and therefore $\epsilon = n$) there is a *unique* solution.

Denote as usual the co-factor of $a_{\mu\nu}$ in $|a|$ by $A_{\mu\nu}$.

If $\nu = q$, $A_{\mu q}a_{\mu\nu} = |a|$, and if $\nu \neq q$, $A_{\mu q}a_{\mu\nu} = 0$. Also since $\delta = n$, $|a| \neq 0$.

Multiplying the equations by $A_{\mu q}$ and adding,

$$(A_{\mu q}a_{\mu\nu})x_\nu + A_{\mu q}b_\mu = 0$$

and this reduces to $|a|x_q = -A_{\mu q}b_\mu \qquad (q = 1 \text{ to } n)$.

Hence if $|b_q|$ denotes the determinant whose elements are those of E with the q^{th} column omitted,

$$x_1 : -x_2 : \ldots : (-1)^{n-1}x_n : (-1)^n = |b_1| : |b_2| : \ldots : |b_n| : |a|$$

Alternatively, $-|a|x_q$ is equal to the determinant formed from $|a|$ by replacing $a_{\mu q}$ by b_μ. In this form the result is known as *Cramer's Rule*.

It has thus been proved that there cannot be more than one solution of the equations, and it is evident by direct substitution that the solution obtained actually satisfies the given equations. Hence if $\delta = \epsilon = n$, a unique solution exists. Another method of finding it is given on p. 443.

(ii) If $\delta = \epsilon < n$, the equations have an *infinity* $(\infty^{n-\epsilon})$ of solutions.

Let F denote the matrix $\begin{bmatrix} a_{11} & a_{12} \ldots a_{1n} & f_1 \\ a_{21} & a_{22} \ldots a_{2n} & f_2 \\ \vdots & \vdots \quad \vdots & \vdots \\ a_{n1} & a_{n2} \ldots a_{nn} & f_n \end{bmatrix}$

which is formed by applying to E the transformation

$$\text{col } (n+1) + x_1 \text{ col } 1 + x_2 \text{ col } 2 + \ldots + x_n \text{ col } n.$$

Since $\epsilon < n$, it follows from p. 423 that there are ϵ rows of E on which the remaining $n - \epsilon$ rows depend. The ϵ corresponding rows of F have the same property, because the same values of the constants κ will serve for F as for E. Therefore there are ϵ of the equations $f_\mu = 0$ whose truth implies that of the others. Further since $\delta = \epsilon$, it is possible to choose ϵ of the variables so

that the determinant formed by their coefficients in these ϵ equations is not zero. If arbitrary values are then assigned to the remaining $n-\epsilon$ variables, a unique solution is determined by these ϵ equations. This solution satisfies the remaining $n-\epsilon$ equations. Thus the given system of equations has an unlimited number $(\infty^{n-\epsilon})$ of solutions.

(iii) If $\delta < \epsilon$, the equations are *inconsistent.*

E must contain a non-zero determinant E_ϵ of order ϵ which involves the column b. The corresponding determinant F_ϵ of F is identically equal to E_ϵ, because the coefficients of x_ν in F_ϵ are determinants of D of order greater than δ or else they are determinants with two columns alike. Expansion by the f column gives $C_\nu f_\nu = F_\epsilon = E_\epsilon \neq 0$.

Here ν has ϵ values, and it follows that no values of the variables exist such that $f_\nu = 0$ for these ϵ values.

To sum up: the solution is unique if $\delta = \epsilon = n$,
there are $\infty^{n-\epsilon}$ solutions if $\delta = \epsilon < n$,
and there is no solution if $\delta \neq \epsilon$.

It can be proved by a similar method that the same statements are true if the number n of the variables is not the same as the number of equations.

Homogeneous Equations.

$f_1 \equiv a_{1\nu} x_\nu = 0$, $f_2 \equiv a_{2\nu} x_\nu = 0, \ldots, f_n \equiv a_{n\nu} x_\nu = 0$ $(\nu = 1 \text{ to } n)$ are n equations for the $n-1$ ratios of the variables, i.e. for $x_1 : x_2 : \ldots : x_n$.

The conditions for the existence of one or more solutions may be deduced from the previous work by putting $b_\nu = 0$. The reader will find it a valuable exercise to establish them for himself. They are as follows:

If δ is the rank of $[a_{ik}]$, then

(i) if $\delta = n$, that is if $|a| \neq 0$, the equations cannot be true unless $x_1 = x_2 = \ldots = x_n = 0$. Thus there is *no solution* for the ratios. In most applications the solution $x_1 = x_2 = \ldots = x_n = 0$ has no significance.

(ii) If $\delta = n-1$, then $|a| = 0$. There are $n-1$ independent rows and there is a *unique* solution for the ratios, viz.

$$x_1 : x_2 : \ldots : x_n = A_{p1} : A_{p2} : \ldots A_{pn}$$

where $A_{\mu\nu}$ is the co-factor of $a_{\mu\nu}$ in $|a_{\mu\nu}|$ and p may have any particular value from 1 to n for which the values of A_{pr} are not all zero. By p. 412, since $|a| = 0$,

$$A_{p1} : A_{p2} : \ldots : A_{pn} = A_{q1} : A_{q2} : \ldots : A_{qn}.$$

(iii) If $\delta < n-1$, there are $n-1-\delta$ of the ratios to which arbitrary values can be assigned, and the others are then uniquely determined. Thus there are $\infty^{n-1-\delta}$ solutions for the ratios. If $n-\delta$ independent solutions are

$$x_1 : x_2 : \ldots : x_n = x_{\rho 1} : x_{\rho 2} : \ldots : x_{\rho n} \quad (\rho = 1 \text{ to } n-\delta)$$

the general solution may be conveniently expressed in the form $x_1 : x_2 : \ldots : x_n = \kappa_\rho x_{\rho 1} : \kappa_\rho x_{\rho 2} : \ldots : \kappa_\rho x_{\rho n}$.

Eliminants. In general a system of m equations connecting n variables is inconsistent if $m > n$.

A relation which must hold between the coefficients so that the equations may be consistent is called an *eliminant* of the system.

For example the $n+1$ equations

$$a_{\mu\nu} x_\nu + b_\mu = 0 \qquad (\mu = 1 \text{ to } n+1,\ \nu = 1 \text{ to } n)$$

have the single eliminant $(a_{11}\ a_{22}\ \ldots\ a_{nn}\ b_{n+1}) = 0$.

Also the n homogeneous equations

$$a_{\mu\nu} x_\nu = 0 \qquad (\mu = 1 \text{ to } n,\ \nu = 1 \text{ to } n)$$

are said to have the eliminant $|a_{\mu\nu}| = 0$ because they cannot be true unless this condition holds (except in the trivial case $x_1 = x_2 = \ldots = x_n = 0$).

EXERCISE XVIIa

A

1. Solve: $\begin{bmatrix} y+z & x+z \\ 7-t & 6-z \end{bmatrix} = \begin{bmatrix} 9-t & 8-t \\ x+y & x+y \end{bmatrix}$

2. If the second-order determinants contained in $\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix}$ are all zero, what can be said about the lines $a_1 x + b_1 y = c_1$, $a_2 x + b_2 y = c_2$?

3. State the ranks of the matrices

(i) $\begin{bmatrix} x & y & z \\ x & y & z \end{bmatrix}$ (ii) $\begin{bmatrix} 0 & 0 & 0 & 0 \\ a & b & c & d \end{bmatrix}$ (iii) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 8 & 6 \end{bmatrix}$

where x, y, z are not all zero and a, b, c, d are not all zero.

4. Prove that the matrix whose rows are 2, 1, 3, 5; 4, 2, 1, 3; 8, 4, 7, 13; 8, 4, -3, -1, is of rank 2.

5. Find whether the following sets are linearly dependent:

(i) 2, 5, 7; 4, 8, 3; 16, 34, 23;

(ii) 2, 9, 5, 1; 10, 39, 47, 11; 1, 3, 8, 2; 13, 51, 79, 19.

6. Prove that the functions $2x+y-2z$, $x-2y+3z$, $x+8y-13z$ are linearly dependent.

Solve the equations in Nos. 7-12 (if consistent) and interpret the results in cartesian geometry of three dimensions.

In Nos. 8-10, find also the values of δ, ϵ. See p. 425.

7. $4x+3y+z=0$, $60x-24y+kz=0$, for $k=360$, $k=-8$, and $k=15$.

8. $2x+3y+z=11$, $x+y+z=6$, $5x-y+10z=34$.

9. $2x+3y+z=11$, $x+y+z=6$, $3x+4y+2z=1$.

10. $2x+3y+z=11$, $x+y+z=6$, $3x+4y+2z=17$.

11. $2x+3y+z=11t$, $x+y+z=6t$, $5x-y+10z=34t$. (See No. 8.)

12. $2x+3y+z=11t$, $x+y+z=6t$, $3x+4y+2z=t$. (See No. 9.)

B

13. If

$$A=\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{bmatrix} \quad B=\begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{bmatrix} \quad C=\begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \\ x_4 & y_4 & z_4 \end{bmatrix}$$

interpret in geometry of two dimensions the following properties

(i) A is of rank 1 (ii) B is of rank 1

(iii) B is of rank 2 (iv) C is of rank 2

In (ii) give also the interpretation for cartesian coordinates in three dimensions.

14. Find the condition for the functions $3x+2y+z$, $12x+y+2z$, $ax+by+cz$ to be linearly dependent.

Solve the equations in Nos. 15-18 (if consistent) and interpret the results in cartesian geometry of three dimensions.

In Nos. 15, 16, find also the values of δ, ϵ. See p. 425.

15. $2x+3y+z=11$, $4x+6y+2z=7$, $3x+4y+2z=1$.

16. $2x+3y+z=10$, $4x+6y+2z=21$, $6x+9y+3z=30$.

17. $x+y=3$, $y+z=2$, $x-z=1$, $3x+2y-z=7$.

18. $x+y+z=9$, $3x-2y+4z=3$.

C

19. Solve $a_\mu x_\mu = b$, $a_\mu^2 x_\mu = b^2$, $a_\mu^3 x_\mu = b^3$ where $\mu = 1, 2, 3$ and a_1, a_2, a_3 are unequal and not zero.

20. Discuss the solution of

$$ax+y+z=1, \quad x+ay+z=a, \quad x+y+az=a^2$$

for different values of a.

Linear Transformations and Matrix Algebra.

The reader is already aware that the theory of complex numbers is developed by applying certain laws of combination to ordered pairs of real numbers (a, b), and he is probably convinced that this excursion into abstract thought is justified by the many useful applications of complex algebra.

A matrix is also a collection of numbers arranged in a certain way and we shall develop an algebra of matrices by laying down laws for their combination. It will not be possible in this book to make much use of matrix algebra, but some applications will be given on pp. 442-448. These applications will at least show that matrix algebra expresses sets of equations in a very concise form and that it can sometimes prove a whole set of results in one piece of work.

The actual law of combination that we adopt is suggested by the consideration of linear transformations. It is sometimes desirable to replace variables x_1, x_2 by new variables y_1, y_2 such that

$$\begin{cases} x_1 = a_{11}y_1 + a_{12}y_2 \\ x_2 = a_{21}y_1 + a_{22}y_2 \end{cases}$$

For example in cartesian plane geometry the transformation for change of axes without change of origin is of this form. Such a transformation is called a linear transformation and $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is called the matrix of the transformation.

If afterwards new variables z_1, z_2 are introduced, and

$$\begin{cases} y_1 = b_{11}z_1 + b_{12}z_2 \\ y_2 = b_{21}z_1 + b_{22}z_2 \end{cases}$$

the combined transformation is expressed by

$$\begin{cases} x_1 = c_{11}z_1 + c_{12}z_2 \\ x_2 = c_{21}z_1 + c_{22}z_2 \end{cases}$$

where $c_{11} = a_{11}b_{11} + a_{12}b_{21}$ $\qquad c_{12} = a_{11}b_{12} + a_{12}b_{22}$

$c_{21} = a_{21}b_{11} + a_{22}b_{21}$ $\qquad c_{22} = a_{21}b_{12} + a_{22}b_{22}$

and it is easily seen that

$$\begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix}.$$

The equations of transformation may be written more shortly as

$$x_\mu = a_{\mu\nu}y_\nu \qquad y_\nu = b_{\nu\rho}z_\rho \qquad (\mu, \nu, \rho = 1, 2)$$

and the combined transformation is $x_\mu = c_{\mu\rho}z_\rho$

where $c_{\mu\rho} = a_{\mu\nu}b_{\nu\rho} = a_{\mu 1}b_{1\rho} + a_{\mu 2}b_{2\rho}$.

This last equation stands for the four equations for c_{11}, c_{12}, c_{21}, c_{22} which are given above.

In the previous example the matrices of the transformations are square. Consider now the transformations given by

$$x_\mu = a_{\mu\nu}y_\nu \qquad (\mu = 1 \text{ to } 4\,;\ \nu = 1, 2)$$
$$y_\nu = b_{\nu\rho}z_\rho \qquad (\nu = 1, 2\,;\ \rho = 1 \text{ to } 3)$$

which are equivalent to

$$x_\mu = c_{\mu\rho}z_\rho \qquad (\mu = 1 \text{ to } 4\,;\ \rho = 1 \text{ to } 3)$$

where $c_{\mu\rho} = a_{\mu\nu}b_{\nu\rho}$ $\qquad (\mu = 1 \text{ to } 4\,;\ \nu = 1, 2\,;\ \rho = 1 \text{ to } 3)$.

This suggests that the product AB of the matrices

$$\mathsf{A} \equiv [a_{\mu\nu}] \quad \text{and} \quad \mathsf{B} \equiv [b_{\nu\rho}]$$

should be defined as the matrix C given by

$$\mathsf{C} \equiv [c_{\mu\rho}] = [a_{\mu\nu}b_{\nu\rho}]$$

But the nature of successive transformations requires that the number of columns in A, being the number of the variables y, should be equal to the number of rows in B.

Except in this case no interpretation is suggested for AB by the theory of transformation, and it is only when the number of columns in A is equal to the number of rows in B that any meaning is assigned to the matrix product AB. This implies that BA is to be distinguished from AB.

Definition of a Matrix Product

If $A=[a_{\mu\nu}]$ and $B=[b_{\nu\rho}]$ ($\mu=1$ to m, $\nu=1$ to n, $\rho=1$ to r) the product AB is defined to be the matrix $[a_{\mu\nu}b_{\nu\rho}]$.

Denoting AB by C or $[c_{\mu\rho}]$ ($\mu=1$ to m, $\rho=1$ to r)

$$c_{\mu\rho}=a_{\mu\nu}b_{\nu\rho}=a_{\mu1}b_{1\rho}+a_{\mu2}b_{2\rho}+\ldots+a_{\mu n}b_{n\rho}.$$

For example

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \\ d_1 & d_2 & d_3 \end{bmatrix} \begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{bmatrix} = \begin{bmatrix} a_1x_1+a_2x_2+a_3x_3 & a_1y_1+a_2y_2+a_3y_3 \\ b_1x_1+b_2x_2+b_3x_3 & b_1y_1+b_2y_2+b_3y_3 \\ c_1x_1+c_2x_2+c_3x_3 & c_1y_1+c_2y_2+c_3y_3 \\ d_1x_1+d_2x_2+d_3x_3 & d_1y_1+d_2y_2+d_3y_3 \end{bmatrix}$$

but $\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{bmatrix} \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \\ d_1 & d_2 & d_3 \end{bmatrix}$ has no meaning because the number of columns of the first matrix is not equal to the number of rows of the second.

If $A=\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

then $AB=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ and $BA=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Thus AB and BA can exist and be different. In this example they are not even conformable which is a first requisite for equality. Also in this example even the determinants $|AB|$ and $|BA|$ are unequal.

If A is an $m \times n$ matrix, the necessary and sufficient condition that AB and BA should both exist is that B should be an $n \times m$ matrix. If A and B are $n \times n$ matrices, then AB and BA both exist. But they are not necessarily equal; for if $A = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 1 \\ 2 & 0 \end{bmatrix}$ then $AB = \begin{bmatrix} 7 & 1 \\ 19 & 3 \end{bmatrix}$ and $BA = \begin{bmatrix} 6 & 11 \\ 2 & 4 \end{bmatrix}$. These are not equal matrices because they have unequal corresponding elements. But in this case of square matrices the determinants $|AB|$ and $|BA|$ are necessarily equal because they are equal to the product of the determinants $|A|$ and $|B|$. This contrasts with the preceding example.

In virtue of the definition of a matrix product, the transformation on p. 433 may be expressed in the form

$$X = AY \qquad Y = BZ$$

where $X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ $Y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ $Z = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$

and A, B are the matrices of the transformations.

The same equations also express the transformation

$$x_\mu = a_{\mu\nu} y_\nu \qquad y_\nu = b_{\nu\rho} z_\rho \qquad (\mu = 1 \text{ to } m,\ \nu = 1 \text{ to } n,\ \rho = 1 \text{ to } r)$$

where $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$ $Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$ $Z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{bmatrix}$.

Sums of Matrices. The *sum* of two *conformable* matrices A and B is defined to be the matrix C given by

$$c_{\mu\nu} = a_{\mu\nu} + b_{\mu\nu}$$

and it is denoted by $A + B$. Thus the sum is found by adding corresponding elements and it only exists for conformable matrices.

Evidently $$A + B = B + A$$

and $$A + (B + C) = (A + B) + C$$

where A, B, C are any three conformable matrices. Thus $A + B + C$ can be written without any ambiguity.

$A+A$ is denoted by $2A$, $A+A+A$ by $3A$, etc.

More generally the product $k[a_{\mu\nu}]$ of a scalar and a matrix is defined to be the matrix $[ka_{\mu\nu}]$. In contrast to this, if $|a_{\mu\nu}|$ is a determinant of order n, $|ka_{\mu\nu}| = k^n |a_{\mu\nu}|$.

The difference $A-B$ between two conformable matrices is defined to be the matrix D given by $A = B+D$.

A *zero* matrix is one in which every element is zero. It is usually denoted by O because the numbers of rows and columns is obvious from the context and because

$$A+O=A=O+A, \quad AO=O=OA.$$

But it must not be concluded from $AB=O$ that one of the matrices A, B must be a zero matrix. See Exercise XVIIb, Nos. 3, 10, 11, 12. For special cases in which the conclusion is legitimate, see p. 440 and Exercise XVIIc, Nos. 31, 32.

The Associative Law of Multiplication

$(AB)C = A(BC)$, provided that the operations are possible.

Suppose that $A=[a_{\lambda\mu}]$, $B=[b_{\mu\nu}]$, $C=[c_{\nu\rho}]$

for $\lambda = 1$ to l, $\mu = 1$ to m, $\nu = 1$ to n, $\rho = 1$ to r.

By definition $$[a_{\lambda\mu}][b_{\mu\nu}] = [a_{\lambda\mu}b_{\mu\nu}]$$

$$\therefore (AB)C = [a_{\lambda\mu}b_{\mu\nu}][c_{\nu\rho}] = [a_{\lambda\mu}b_{\mu\nu}c_{\nu\rho}].$$

Similarly $$A(BC) = [a_{\lambda\mu}][b_{\mu\nu}c_{\nu\rho}] = [a_{\lambda\mu}b_{\mu\nu}c_{\nu\rho}]$$

$$\therefore (AB)C = A(BC)$$

and it follows that ABC can be written without ambiguity.

If A is a square matrix, AA exists and it is denoted by A^2. Also, since $(AA)A = A(AA)$, the notation AAA or A^3 may be used, etc.

The Distributive Laws

$(A+B)C = AC+BC$, provided that the operations are possible.

A, B must be conformable and must have the same number of columns as C has rows.

Suppose that $A=[a_{\lambda\mu}]$, $B=[b_{\lambda\mu}]$, $C=[c_{\mu\nu}]$

for $\lambda = 1$ to l, $\mu = 1$ to m, $\nu = 1$ to n.

By definition $$(A+B)C = [a_{\lambda\mu}+b_{\lambda\mu}][c_{\mu\nu}]$$

$$= [(a_{\lambda\mu}+b_{\lambda\mu})c_{\mu\nu}] = [a_{\lambda\mu}c_{\mu\nu}+b_{\lambda\mu}c_{\mu\nu}]$$

$$= [a_{\lambda\mu}c_{\mu\nu}] + [b_{\lambda\mu}c_{\mu\nu}] = AC+BC.$$

Similarly it may be proved that $A(B+C)=AB+AC$.

It is most important to remember that multiplication of matrices is not commutative and that $AB=O$ does not imply $A=O$ or $B=O$. But the following laws apply:

$$A+B=B+A \qquad A+(B+C)=(A+B)+C$$

$$A(BC)=(AB)C$$

$$(A+B)C=AC+BC$$

$$A(B+C)=AB+AC$$

Hence it follows for example that

$$(A+B)(C+D)=AC+AD+BC+BD$$

where the order of the factors is preserved.

EXERCISE XVIIb

A

In Nos. 1-4 give when possible the values of $A+B$, AB, BA.

1. $A=\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}$, $B=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$

2. $A=\begin{bmatrix}1 & 2 & 3\\ 1 & 3 & 6\end{bmatrix}$, $B=\begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 3\end{bmatrix}$

3. $A=\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}$, $B=\begin{bmatrix}b & b\\ -a & -a\end{bmatrix}$

4. $A=\begin{bmatrix}0 & 1\\ 1 & 2\\ 2 & 3\\ 3 & 4\end{bmatrix}$, $B=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 3 & 5 & 7\end{bmatrix}$

5. Write in full the matrices $[a_{\mu\nu}]$ and $[a_{\nu\mu}]$ when
(i) $\mu=1, 2$; $\nu=1, 2$. (ii) $\mu=1, 2$; $\nu=1, 2, 3$.

6. A has x rows and $x+5$ columns, B has y rows and $11-y$ columns, and AB, BA exist. Find x and y.

7. Write $\begin{bmatrix}x & y & z\end{bmatrix}\begin{bmatrix}a & h & g\\ h & b & f\\ g & f & c\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}$ as a single matrix.

8. If $\mathsf{A}=\begin{bmatrix} k & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & k \end{bmatrix}$, $\mathsf{B}=[b_{\mu\nu}]$ $(\mu, \nu = 1 \text{ to } 3)$, prove that $\mathsf{AB}=\mathsf{BA}=k\mathsf{B}$.

9. Expand $(\mathsf{A}+\mathsf{B})^2$, stating when this can be done.

10. Evaluate $\begin{bmatrix} 0 & c & -b \\ -c & 0 & a \\ b & -a & 0 \end{bmatrix}\begin{bmatrix} a^2 & ab & ac \\ ba & b^2 & bc \\ ca & cb & c^2 \end{bmatrix}$

B

In Nos. 11-14 give when possible the values of $\mathsf{A}+\mathsf{B}$, AB, BA

11. $\mathsf{A}=\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$, $\mathsf{B}=\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$

12. $\mathsf{A}=\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$, $\mathsf{B}=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

13. $\mathsf{A}=\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$, $\mathsf{B}=\begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}$

14. $\mathsf{A}=\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$, $\mathsf{B}=\begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix}$

15. Verify (see p. 410):

(i) $[a_1 \quad a_2 \dots a_n]\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = [a \mid b]$,

(ii) $\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}\begin{bmatrix} p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \end{bmatrix} = \begin{bmatrix} a \mid p & a \mid q \\ b \mid p & b \mid q \end{bmatrix}$.

16. Verify that $\mathsf{A}(\mathsf{B}+\mathsf{C})=\mathsf{AB}+\mathsf{AC}$ provided that the operations are possible and state the conditions for this to be so.

17. Expand $(\mathsf{A}+\mathsf{B})(\mathsf{A}-\mathsf{B})$, stating when this can be done.

C

18. If $\mathsf{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $\mathsf{i}=\begin{bmatrix}\delta & 0\\ 0 & -\delta\end{bmatrix}$, $\mathsf{j}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$, $\mathsf{k}=\begin{bmatrix}0 & \delta\\ \delta & 0\end{bmatrix}$

where $\delta^2=-1$, show that $\mathsf{i}^2=\mathsf{j}^2=\mathsf{k}^2=-\mathsf{I}$ and $\mathsf{ij}=\mathsf{k}$. Deduce that $\mathsf{ik}=-\mathsf{j}$, $\mathsf{kj}=-\mathsf{i}$, $\mathsf{ki}=\mathsf{j}$ and obtain similar results for ji and jk.

19. With the notation of No. 18, if $\mathsf{Q}=a\mathsf{I}+b\mathsf{i}+c\mathsf{j}+d\mathsf{k}$ and $\bar{\mathsf{Q}}=a\mathsf{I}-b\mathsf{i}-c\mathsf{j}-d\mathsf{k}$ where a, b, c, d are scalar, Q and $\bar{\mathsf{Q}}$ are called *conjugate quaternions*, and $n(\mathsf{Q})$, $\equiv a^2+b^2+c^2+d^2$, is called the *norm* of Q.

(i) Show that $\mathsf{Q}=\begin{bmatrix}a+\delta b & c+\delta d\\ -c+\delta d & a-\delta b\end{bmatrix}$ and express $\bar{\mathsf{Q}}$ as a two-rowed matrix.

(ii) Prove that $\mathsf{Q}\bar{\mathsf{Q}}=\bar{\mathsf{Q}}\mathsf{Q}=n(\mathsf{Q})\mathsf{I}$.

(iii) If P, Q are quaternions, prove that PQ is a quaternion with $\bar{\mathsf{Q}}\bar{\mathsf{P}}$ for conjugate, and that $n(\mathsf{PQ})=n(\mathsf{P})n(\mathsf{Q})$.

20. If $a_{\lambda\mu}=\lambda+\mu$ and $b_{\mu\nu}=\mu-\nu$ where $\lambda=1, 2$; $\mu=1, 2, 3$; $\nu=1, 2$, find the values of $[a_{\lambda\mu}]+[b_{\nu\mu}]$ and $[a_{\lambda\mu}][b_{\mu\nu}]$.

21. If A, B, C are the elements of matrices of n rows with a, b, c columns where $a+b+c\mp 2n$, and O indicates zero elements, prove that $\begin{vmatrix}\mathrm{A} & \mathrm{B} & \mathrm{O}\\ \mathrm{A} & \mathrm{O} & \mathrm{C}\end{vmatrix}=(-1)^{n+c+ab}\begin{vmatrix}\mathrm{B} & \mathrm{A} & \mathrm{O}\\ \mathrm{B} & \mathrm{O} & \mathrm{C}\end{vmatrix}$

where the determinants are composed of the elements in the positions shown.

Square Matrices. The matrix $[a_{\mu\nu}]$ ($\mu=1$ to m, $\nu=1$ to n) is called *square* if $m=n$, and is then called *singular* when $|a|=0$. When $|a|\neq 0$, the matrix is called *non-singular* or *regular*.

The square matrix defined by

$$a_{\mu\nu}=0 \text{ if } \mu\neq\nu, \quad \text{and} \quad a_{\mu\mu}=1 \qquad (\mu, \nu=1 \text{ to } n)$$

is called a *unit* matrix and is denoted by I_n.

The square matrix defined by

$$a_{\mu\nu}=0 \text{ if } \mu\neq\nu, \quad \text{and} \quad a_{\mu\mu}=k \qquad (\mu, \nu=1 \text{ to } n)$$

is called a *scalar* matrix. It can be denoted by $k\mathsf{I}_n$ without conflicting with the definition of $k[a_{\mu\nu}]$ on p. 434.

The scalar matrix is a device for replacing a scalar by a matrix, and there is an exact correspondence between the algebra of scalar matrices and ordinary algebra. This may be compared with the correspondence between real and x-axal numbers.

In unit and scalar matrices the suffix n is sometimes omitted, leaving the number of rows and columns to be inferred from the context as in the case of zero matrices.

It is easily verified that if A is a matrix with m rows and n columns,

$$AI_n = A = I_m A$$

Hence if $AI_n = O$, then $A = O$,

and if $AI_n = BI_n$, then $A = B$

also if the product AB exists, $AI_n B = AB$. Thus in any piece of manipulation a unit matrix which occurs in a product can be omitted.

The Transposed Matrix. The matrix whose rows are identical with the columns of a matrix A has been (see p. 422) called the *transposed* of A and is denoted by A′. A square matrix may be equal to its transposed; it is then called symmetrical.

The transposed of A′ is A, i.e. $(A')' = A$.

It follows from the definition of a product that if AB exists,

$$(AB)' = B'A'.$$

Hence if ABC exists,

$$(ABC)' = (AB.C)'$$
$$= C'(AB)' = C'B'A'$$

and similarly $(A_1 A_2 \dots A_n)' = A_n' A_{n-1}' \dots A_1'$.

The Adjoint and the Inverse. The *adjoint* of a *square* matrix $[a_{\mu\nu}]$ is defined to be the matrix $[b_{\mu\nu}]$, where $b_{\mu\nu}$ is the co-factor of $a_{\nu\mu}$ in the determinant $|a|$. This co-factor is formed by striking out the ν^{th} row and the μ^{th} column and multiplying by $(-1)^{\mu+\nu}$ as explained on p. 401, and it is denoted by $A_{\nu\mu}$.

For example the adjoint of $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ is not

$$\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{bmatrix}$$

and A_{21} denotes $-\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix}$.

Provided that the square matrix $\mathsf{A} \equiv [a_{\mu\nu}]$ is non-singular, it also has an *inverse* defined as $[c_{\mu\nu}]$, where $c_{\mu\nu} = A_{\nu\mu} \div |a|$, and denoted by A^{-1}. These definitions of adjoint and inverse matrices should be contrasted with those of adjugate and reciprocal determinants given in Chapter XVI. Mathematical writers differ about the precise meanings of these terms.

If $\mathsf{A} = [a_{\lambda\mu}]$ and $\mathsf{A}^{-1} = [c_{\mu\nu}]$, the definition gives $c_{\mu\nu} = A_{\nu\mu} \div |a|$.

Hence $$\mathsf{A}\mathsf{A}^{-1} = [a_{\lambda\mu} c_{\mu\nu}] = [a_{\lambda\mu} A_{\nu\mu} \div |a|]$$

But by equation (12), p. 405,

$$a_{\lambda\mu} A_{\nu\mu} = |a| \text{ if } \lambda = \nu \quad \text{and} \quad a_{\lambda\mu} A_{\nu\mu} = 0 \text{ if } \lambda \neq \nu.$$

Hence $\mathsf{A}\mathsf{A}^{-1} = \mathsf{I}_n$.

By writing $\mathsf{A} = [a_{\lambda\mu}]$ and $\mathsf{A}^{-1} = [d_{\nu\lambda}]$ where $d_{\nu\lambda} = A_{\lambda\nu} \div |a|$ it may be proved similarly that $\mathsf{A}^{-1}\mathsf{A} = \mathsf{I}_n$.

Thus $\mathsf{A}\mathsf{A}^{-1} = \mathsf{I}_n = \mathsf{A}^{-1}\mathsf{A}$. This is a case in which the commutative law of multiplication holds good.

If A is a non-singular (square) matrix and AB exists and is equal to C, then $\mathsf{B} = \mathsf{A}^{-1}\mathsf{C}$.

For $$\mathsf{A}^{-1}\mathsf{C} = \mathsf{A}^{-1}\mathsf{A}\mathsf{B} = \mathsf{I}\mathsf{B} = \mathsf{B}.$$

If A is a non-singular (square) matrix and BA exists and is equal to D, then $\mathsf{B} = \mathsf{D}\mathsf{A}^{-1}$.

For $$\mathsf{D}\mathsf{A}^{-1} = \mathsf{B}\mathsf{A}\mathsf{A}^{-1} = \mathsf{B}\mathsf{I} = \mathsf{B}.$$

In particular, since $\mathsf{A}\mathsf{A}^{-1} = \mathsf{I}$, it follows that

$$\mathsf{A} = \mathsf{I}(\mathsf{A}^{-1})^{-1} = (\mathsf{A}^{-1})^{-1}.$$

Hence the *inverse of the inverse* of a non-singular (square) matrix is the matrix itself.

Also the *inverse of the transposed* matrix of a non-singular (square) matrix is equal to the *transposed of the inverse.*

For $(AA^{-1})' = I' = I, \quad \therefore (A^{-1})'A' = I.$

Hence $(A^{-1})' = I(A')^{-1} = (A')^{-1}.$

If A and B are conformable non-singular (square) matrices, then

$$(AB)^{-1} = B^{-1}A^{-1}.$$

For $(AB)(AB)^{-1} = I, \quad \therefore A.B(AB)^{-1} = I,$

$$\therefore B(AB)^{-1} = A^{-1}I = A^{-1}$$

$$\therefore (AB)^{-1} = B^{-1}A^{-1}.$$

Similarly it can be proved that if $A_1, A_2, \ldots, A_n$ are conformable non-singular (square) matrices,

$$(A_1 A_2 \ldots A_n)^{-1} = A_n^{-1} A_{n-1}^{-1}, \ldots A_1^{-1}.$$

Fore and Aft Division

If A is a regular matrix with n rows and n columns, and B is another matrix, a meaning may be assigned to $B \div A$ by finding either P such that $AP = B$, or Q such that $QA = B$.

$AP = B$ is equivalent to $P = A^{-1}B$ and the existence of P requires that B should have n rows.

$QA = B$ is equivalent to $Q = BA^{-1}$ and the existence of Q requires that B should have n columns.

If B has n rows and n columns, both P and Q exist. There are then two quotients. These are distinguished as the *fore* and *aft* quotients and on account of the failure of the commutative law of multiplication they are in general different.

Example 1. Solve the n equations given by $AX = B$

where $A = \begin{bmatrix} a_{11} & a_{12} \ldots a_{1n} \\ a_{21} & a_{22} \ldots a_{2n} \\ \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2} \ldots a_{nn} \end{bmatrix} \quad X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$

and A is regular.

The equations are

$$a_{\mu 1}x_1 + a_{\mu 2}x_2 + \ldots + a_{\mu n}x_n = b_\mu \qquad (\mu = 1 \text{ to } n)$$

and except for the signs of b_μ are the same as those on p. 425.

$\mathsf{AX} = \mathsf{B}$. Therefore by taking the fore quotient,

$\mathsf{X} = \mathsf{A}^{-1}\mathsf{B}$.

Since $\mathsf{A}^{-1} = [c_{\mu\nu}]$ where $c_{\mu\nu} = A_{\nu\mu} \div |a|$,

the solution may be written

$$x_\mu = A_{\nu\mu} b_\nu \div |a| \qquad (\mu = 1 \text{ to } n).$$

Example 2. If $l_1^2 + m_1^2 + n_1^2 = l_2^2 + m_2^2 + n_2^2 = l_3^2 + m_3^2 + n_3^2 = 1$ and $l_1 l_2 + m_1 m_2 + n_1 n_2 = l_2 l_3 + m_2 m_3 + n_2 n_3 = l_3 l_1 + m_3 m_1 + n_3 n_1 = 0$, prove that $l_1^2 + l_2^2 + l_3^2 = 1$, $m_1 n_1 + m_2 n_2 + m_3 n_3 = 0$, etc.

Let $\mathsf{A} = \begin{bmatrix} l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \\ l_3 & m_3 & n_3 \end{bmatrix}$. Then $\mathsf{A}' = \begin{bmatrix} l_1 & l_2 & l_3 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{bmatrix}$

and $\mathsf{AA}' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \mathsf{I}_3$

Hence $\mathsf{A}'\mathsf{A} = \mathsf{A}'\mathsf{I}_3(\mathsf{A}')^{-1} = \mathsf{A}'(\mathsf{A}')^{-1} = \mathsf{I}_3$, i.e.

$$\begin{bmatrix} l_1^2 + l_2^2 + l_3^2 & l_1 m_1 + l_2 m_2 + l_3 m_3 & l_1 n_1 + l_2 n_2 + l_3 n_3 \\ m_1 l_1 + m_2 l_2 + m_3 l_3 & m_1^2 + m_2^2 + m_3^2 & m_1 n_1 + m_2 n_2 + m_3 n_3 \\ n_1 l_1 + n_2 l_2 + n_3 l_3 & n_1 m_1 + n_2 m_2 + n_3 m_3 & n_1^2 + n_2^2 + n_3^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and, from the equality of the nine pairs of corresponding elements, the results follow.

The interpretation in geometry of three dimensions of the result of Example 2 is that the direction cosines of three mutually perpendicular lines satisfy the given relations; and (l_1, l_2, l_3), (m_1, m_2, m_3), (n_1, n_2, n_3), being the direction cosines of the original axes referred to the other three lines as axes, must satisfy the required relations.

Inverse Transformations. We have seen that a linear transformation (T) from $x_1, x_2, \dots, x_n$ to $y_1, y_2, \dots, y_n$ can be expressed by a matrix equation $\mathsf{X} = \mathsf{A}\mathsf{Y}$ where

$$\mathsf{X}' = [x_1 x_2 \dots x_n] \quad \mathsf{Y}' = [y_1 y_2 \dots y_n] \quad \mathsf{A} = [a_{\mu\nu}] \qquad (\mu, \nu = 1 \text{ to } n).$$

If A is regular, it follows that $\mathsf{Y} = \mathsf{A}^{-1}\mathsf{X}$. This matrix equation gives the inverse transformation (T^{-1}) from $y_1, y_2, \dots, y_n$ to $x_1, x_2, \dots, x_n$, i.e. it gives the n equations for y_μ in terms of x_μ which could be found less concisely by solving the n equations of the transformation T.

Cogredience and Contragredience. Sets of variables to which the same transformation applies are called *cogredient*. For example in the change from one system of homogeneous coordinates in 2-dimensional geometry to another system, the point coordinates x_μ ($\mu = 1$ to 3) are transformed into y_μ by equations

$$\mathsf{X} = \mathsf{A}\mathsf{Y} \quad \text{i.e.} \quad x_\mu = a_{\mu\nu} y_\nu \qquad (\mu, \nu = 1 \text{ to } 3).$$

This transformation applies to all points, and point coordinates are therefore cogredient. But it will be found that this transformation induces in the corresponding line coordinates u_μ of a line $u_\mu x_\mu = 0$ another transformation, and that this transformation has a matrix which is in general different from A, so that the line coordinates are not cogredient with the point coordinates.

Substituting for x_μ from $\mathsf{X} = \mathsf{A}\mathsf{Y}$,

$$u_\mu x_\mu = u_\mu a_{\mu\nu} y_\nu = v_\nu y_\nu, \quad \text{where } v_\nu = a_{\mu\nu} u_\mu.$$

But $v_\nu = a_{\mu\nu} u_\mu$ is equivalent to $\mathsf{V} = \mathsf{A}'\mathsf{U}$

$$\text{where} \quad \mathsf{V}' = [v_1 v_2 v_3], \quad \mathsf{U}' = [u_1 u_2 u_3],$$

and A is regular, $\quad \therefore \ \mathsf{U} = (\mathsf{A}')^{-1}\mathsf{V}.$

Hence the matrix of the induced transformation is $(\mathsf{A}')^{-1}$ and this is in general different from A.

Conversely if $\quad \mathsf{U} = (\mathsf{A}')^{-1}\mathsf{V},$

$$\mathsf{V} = \mathsf{A}'\mathsf{U}, \qquad \therefore \ \mathsf{V}' = \mathsf{U}'\mathsf{A}$$

Hence $\qquad [u_\mu x_\mu] \equiv \mathsf{U}'\mathsf{X} = \mathsf{U}'\mathsf{A}\mathsf{Y} = \mathsf{V}'\mathsf{Y} \equiv [v_\nu y_\nu].$

Two sets such as x_μ and u_μ which are changed (into y_μ and v_μ) by transformations whose matrices are A and $(\mathsf{A}')^{-1}$ are called

contragredient sets. Their inner product $u_\mu x_\mu$ is invariant. It is shown above that the point and line coordinates are contragredient. Another example of contragredience is given in Example 3. When $\mathsf{A} = (\mathsf{A}')^{-1}$, the sets are both cogredient and contragredient. (See p. 446.)

Note. The definitions and algebra in the preceding section are applicable to sets of n variables with $\mu, \nu = 1$ to n.

Example 3. If $u_\mu = \dfrac{\partial}{\partial x_\mu}$ ($\mu = 1$ to 3), show that the sets (x_μ), (u_μ) are contragredient for the transformation

$$x_\mu = a_{\mu\nu} y_\nu \quad (\mu, \nu = 1 \text{ to } 3), \quad |a_{\mu\nu}| \neq 0.$$

The given transformation is of the form $\mathsf{X} = \mathsf{AY}$ and it is to be proved that $\mathsf{U} = (\mathsf{A}')^{-1}\mathsf{V}$, where

$$\mathsf{U}' = [u_1 u_2 u_3], \quad \mathsf{V}' = [v_1 v_2 v_3] \quad \text{and} \quad v_\mu = \frac{\partial}{\partial y_\mu}.$$

$$\frac{\partial}{\partial y_\mu} = \frac{\partial}{\partial x_1}\frac{\partial x_1}{\partial y_\mu} + \frac{\partial}{\partial x_2}\frac{\partial x_2}{\partial y_\mu} + \frac{\partial}{\partial x_3}\frac{\partial x_3}{\partial y_\mu}$$

$$\therefore \quad v_\mu = u_1 a_{1\mu} + u_2 a_{2\mu} + u_3 a_{3\mu} = u_\nu a_{\nu\mu}$$

and

$$\mathsf{A}'\mathsf{U} = \begin{bmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \mathsf{V}.$$

$$\therefore \quad \mathsf{U} = (\mathsf{A}')^{-1}\mathsf{V}$$

Orthogonal Matrices and Transformations

A matrix A is called *orthogonal* if $\mathsf{A}'\mathsf{A} = \mathsf{I}$.

Since $|\mathsf{A}|^2 = |\mathsf{A}'||\mathsf{A}| = 1$, an orthogonal matrix is regular, and it follows that $\mathsf{A}' = \mathsf{A}^{-1}$ and $\mathsf{A}\mathsf{A}' = \mathsf{I}$.

When the matrix A of a transformation $\mathsf{X} = \mathsf{AY}$ (see p. 435), from variables x_μ to variables y_μ ($\mu = 1$ to n), is orthogonal, the transformation is also called *orthogonal*.

Since $\mathsf{X} = \mathsf{AY}$, $\mathsf{X}' = \mathsf{Y}'\mathsf{A}'$, and $\mathsf{A}'\mathsf{A} = \mathsf{I}$, it follows that $\mathsf{X}'\mathsf{X} = \mathsf{Y}'\mathsf{Y}$

i.e. $$x_1^2 + x_2^2 + \ldots + x_n^2 = y_1^2 + y_2^2 + \ldots + y_n^2.$$

This property, regarded as an identity, might have been taken as the definition of an orthogonal transformation. For direct substitution of $a_{\mu p}y_p$ for x_μ gives, by equating coefficients,

$$a_{\mu p}a_{\mu p}=1 \qquad a_{\mu p}a_{\mu q}=0 \quad (p\neq q)$$

where p, q take the values 1, 2, ... , n. These equations express $\mathsf{A'A}=\mathsf{I}$. In the special case of $n=3$, they are the equations of Example 2.

When the matrix A is orthogonal, $(\mathsf{A'})^{-1}=\mathsf{A}$ and the point and line coordinates (see p. 444) are cogredient and contragredient.

Miscellaneous Applications. The reader will be aware of the importance of the homogeneous quadratic form

$$ax_1^2+bx_2^2+cx_3^2+2fx_2x_3+2gx_3x_1+2hx_1x_2.$$

If A is the matrix $\begin{bmatrix} a & h & g \\ h & b & f \\ g & f & c \end{bmatrix}$ the form may be written as $[x_1\ x_2\ x_3]\mathsf{A}[x_1\ x_2\ x_3]'$ or as $\mathsf{X'AX}$.

Similarly the general homogeneous quadratic form in n variables is associated with a symmetrical matrix A of n rows and n columns and may be written as $[x_1\ x_2 \dots x_n]\mathsf{A}[x_1\ x_2 \dots x_n]'$ or as $\mathsf{X'AX}$.

The determinant $|\mathsf{A}|$ is of importance in the theory of quadratic forms. If a linear transformation $\mathsf{X}=\mathsf{MY}$, where

$$\mathsf{X'}=[x_1\ x_2 \dots x_n] \qquad \mathsf{Y'}=[y_1\ y_2 \dots y_n]$$

is applied to the quadratic form $\mathsf{X'AX}$, then this form becomes $(\mathsf{MY})'\mathsf{AMY}$, i.e. $\mathsf{Y'M'AMY}$, or $\mathsf{Y'BY}$ where $\mathsf{B}=\mathsf{M'AM}$.

B is the matrix of the new form $\mathsf{Y'BY}$. Also $|\mathsf{B}|=|\mathsf{A}||\mathsf{M}|^2$.

If $\varphi\equiv\mathsf{X'AX}$ and $\psi\equiv\mathsf{X'BX}$ are two quadratic forms in

$$x_1, x_2, \dots, x_n,$$

then $\varphi+\lambda\psi\equiv\mathsf{X'CX}$, where $\mathsf{C}=\mathsf{A}+\lambda\mathsf{B}$

and if this form is transformed by $\mathsf{X}=\mathsf{MY}$, it becomes $\mathsf{Y'DY}$, where by the preceding paragraph

$$\mathsf{D}=\mathsf{M'CM} \quad \text{and} \quad |\mathsf{D}|=|\mathsf{C}||\mathsf{M}|^2.$$

Thus the roots of $|\mathsf{C}|=0$, an equation of degree n in λ, are the same as the roots of $|\mathsf{D}|=0$.

This is a familiar result for $n=3$ and it has been proved here for the general case as shortly as it could be proved for $n=3$.

In real algebra the cubic equation in λ

$$\begin{vmatrix} a-\lambda & h & g \\ h & b-\lambda & f \\ g & f & c-\lambda \end{vmatrix} = 0$$

has three roots. (See p. 286.)

Also if A is a symmetrical matrix of real elements which has n rows, then the equation $|A-\lambda I_n|=0$ has n roots.

We prove here the following more general result:

If A *is a matrix* $[a_{\mu\nu}]$ *whose elements* $a_{\mu\nu}$ *are complex numbers* $b_{\mu\nu}+ic_{\mu\nu}$ *such that* $b_{\mu\nu}+ic_{\mu\nu}=b_{\nu\mu}-ic_{\nu\mu}$ *then all the roots of* $|A-\lambda I_n|=0$ *are* x*-axal.*

Using a bar to denote a conjugate complex number, the hypothesis may be expressed as $a_{\mu\nu}=\bar{a}_{\nu\mu}$, or as $\bar{A}=A'$ if $\bar{A}$ is the matrix whose elements are the conjugates of the corresponding elements of A. Let λ denote any root of $|A-\lambda I_n|=0$; then the n linear equations implied by

$$A[x_1\ x_2 \dots x_n]' - \lambda[x_1\ x_2 \dots x_n]' = 0$$

are satisfied by a set of values of $x_1, x_2, \dots, x_n$ not all zero. For these values

$$[\bar{x}_1\ \bar{x}_2 \dots \bar{x}_n]A[x_1\ x_2 \dots x_n]' = [\bar{x}_1\ \bar{x}_2 \dots \bar{x}_n]\lambda[x_1\ x_2 \dots x_n]'$$
$$= [\bar{x}_1\ \bar{x}_2 \dots \bar{x}_n]\begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{bmatrix} = [\lambda k]$$

where k is a sum of squares of x-axal numbers and is not zero. But $[\lambda k]$ being a one-term matrix is unaltered by transposition; hence $[\bar{x}_1\ \bar{x}_2 \dots \bar{x}_n]A[x_1\ x_2 \dots x_n]'$ is unaltered by transposition and is therefore equal to the matrix

$$[x_1\ x_2 \dots x_n]A'[\bar{x}_1\ \bar{x}_2 \dots \bar{x}_n]'.$$

But the substitution of $-i$ for i also changes it into this same matrix in virtue of the hypothesis $\bar{A}=A'$. Hence the substitution leaves λk unaltered, and therefore, since $k\neq 0$, λ is x-axal.

This proof can alternatively be expressed by means of dummy suffixes as follows.

If λ is a root of $|A - \lambda I_n| = 0$, the equations $a_{\mu\nu}x_\nu - \lambda x_\mu = 0$ have a non-zero solution for x_μ.

Multiply by $\bar{x}_\mu$ and add:

$$\bar{x}_\mu a_{\mu\nu} x_\nu = \lambda \bar{x}_\mu x_\mu = \lambda k \quad (k > 0).$$

Changing i into $-i$, the expression which is equal to λk becomes $x_\mu \bar{a}_{\mu\nu} \bar{x}_\nu$. By hypothesis this is equal to $x_\mu a_{\nu\mu} \bar{x}_\nu$, and, by exchange of dummy suffixes, to $x_\nu a_{\mu\nu} \bar{x}_\mu$. Hence it is unaltered; and therefore λ is x-axal.

Two Properties of Determinants

I If $A \equiv [a_{\mu\nu}]$ and $B \equiv [b_{\nu\rho}]$ $(\mu = 1 \text{ to } m,\ \nu = 1 \text{ to } n,\ \rho = 1 \text{ to } m)$ and if $m > n$ and $AB = C$, then $|C| = 0$.

By the definition of C and the product theorem for determinants:

$$|C| = \begin{vmatrix} a_{11} & \dots & a_{1n} & 0 & \dots & 0 \\ a_{21} & \dots & a_{2n} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} & 0 & \dots & 0 \end{vmatrix} \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nm} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{vmatrix}$$

where there are $m - n$ columns of zeros in the first determinant and $m - n$ rows of zeros in the second. Hence $|C| = 0$.

For example

$$\begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \\ z_1 & z_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} = \begin{bmatrix} a_1x_1 + a_2x_2 & b_1x_1 + b_2x_2 & c_1x_1 + c_2x_2 \\ a_1y_1 + a_2y_2 & b_1y_1 + b_2y_2 & c_1y_1 + c_2y_2 \\ a_1z_1 + a_2z_2 & b_1z_1 + b_2z_2 & c_1z_1 + c_2z_2 \end{bmatrix}$$

$$\therefore \begin{vmatrix} a_1x_1 + a_2x_2 & b_1x_1 + b_2x_2 & c_1x_1 + c_2x_2 \\ a_1y_1 + a_2y_2 & b_1y_1 + b_2y_2 & c_1y_1 + c_2y_2 \\ a_1z_1 + a_2z_2 & b_1z_1 + b_2z_2 & c_1z_1 + c_2z_2 \end{vmatrix} = 0.$$

II If $\mathsf{A} \equiv [a_{\mu\nu}]$ and $\mathsf{B} \equiv [b_{\nu\rho}]$ ($\mu = 1$ to m, $\nu = 1$ to n, $\rho = 1$ to m) and if $m < n$ and $\mathsf{AB} = \mathsf{C}$, then $|\mathsf{C}|$ is equal to the sum of the products of corresponding determinants of order m taken from A and B.

For example the identity on p. 370 follows from II, thus

$$\begin{bmatrix} a_1 & a_2 \dots a_n \\ b_1 & b_2 \dots b_n \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \\ \vdots & \vdots \\ a_n & b_n \end{bmatrix} = \begin{bmatrix} \Sigma a^2 & \Sigma ab \\ \Sigma ab & \Sigma b^2 \end{bmatrix}$$

$$\therefore \begin{vmatrix} \Sigma a^2 & \Sigma ab \\ \Sigma ab & \Sigma b^2 \end{vmatrix} = \Sigma \begin{vmatrix} a_r & a_s \\ b_r & b_s \end{vmatrix} \begin{vmatrix} a_r & b_r \\ a_s & b_s \end{vmatrix} = \Sigma (a_r b_s - a_s b_r)^2.$$

The general theorem may be proved as follows:

$$|\mathsf{C}| = |c_{\mu\rho}| = \epsilon_{\rho_1 \rho_2 \dots \rho_m} c_{1\rho_1} c_{2\rho_2} \dots c_{m\rho_m}$$

$$= \epsilon_{\rho_1 \rho_2 \dots \rho_m} (a_{1\nu_1} b_{\nu_1 \rho_1})(a_{2\nu_2} b_{\nu_2 \rho_2}) \dots (a_{m\nu_m} b_{\nu_m \rho_m})$$

where each ν takes the values 1 to n. This may be rearranged as $|\mathsf{C}| = (a_{1\nu_1} a_{2\nu_2} \dots a_{m\nu_m})(\epsilon_{\rho_1 \rho_2 \dots \rho_m} b_{\nu_1 \rho_1} b_{\nu_2 \rho_2} \dots b_{\nu_m \rho_m})$ (see p. 394) and in evaluating the second bracket $\nu_1, \nu_2, \dots, \nu_m$ are fixed and are any particular selection of m numbers from the numbers 1 to n. Denote this selection when arranged in ascending order by $\lambda_1, \lambda_2, \dots, \lambda_m$ and denote the determinant $(b_{\lambda_1 1} b_{\lambda_2 2} \dots b_{\lambda_m m})$ by $|b_m|$.

Then from equation (5), p. 399

$$\epsilon_{\rho_1 \rho_2 \dots \rho_m} b_{\nu_1 \rho_1} b_{\nu_2 \rho_2} \dots b_{\nu_m \rho_m} = \delta^{\lambda_1 \lambda_2 \dots \lambda_m}_{\nu_1 \nu_2 \dots \nu_m} |b_m|$$

Here δ must be used instead of ϵ because $\nu_1, \nu_2, \dots, \nu_m$ are not the numbers 1 to m but a selection of any m numbers from 1 to n.

Also for the particular set of values $\nu_1, \nu_2, \dots, \nu_m$

$$(a_{1\nu_1} a_{2\nu_2} \dots a_{m\nu_m}) \delta^{\lambda_1 \lambda_2 \dots \lambda_m}_{\nu_1 \nu_2 \dots \nu_m} = (a_{1\lambda_1} a_{2\lambda_2} \dots a_{m\lambda_m})$$

$$= |a_m|, \text{ say.}$$

Hence $|\mathsf{C}|$ is equal to the sum of the $\binom{n}{m}$ products $|a_m|\ |b_m|$ obtained by taking all possible selections $\nu_1, \nu_2, \dots, \nu_m$ from the n numbers 1 to n.

Example 4. Prove the identity

$$(a_1x_1+b_1y_1+c_1z_1)(a_2x_2+b_2y_2+c_2z_2) - (a_2x_1+b_2y_1+c_2z_1)(a_1x_2+b_1y_2+c_1z_2) = \Sigma\{(b_1c_2-b_2c_1)(y_1z_2-y_2z_1)\}.$$

$$\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \\ z_1 & z_2 \end{bmatrix} = \begin{bmatrix} a_1x_1+b_1y_1+c_1z_1 & a_1x_2+b_1y_2+c_1z_2 \\ a_2x_1+b_2y_1+c_2z_1 & a_2x_2+b_2y_2+c_2z_2 \end{bmatrix}$$

Hence by II

$$\begin{vmatrix} a_1x_1+b_1y_1+c_1z_1 & a_1x_2+b_1y_2+c_1z_2 \\ a_2x_1+b_2y_1+c_2z_1 & a_2x_2+b_2y_2+c_2z_2 \end{vmatrix} = \Sigma \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix} \begin{vmatrix} y_1 & y_2 \\ z_1 & z_2 \end{vmatrix}$$

from which the result follows.

If the order of multiplication is reversed, the determinant of the product is zero as in I.

EXERCISE XVIIc

A

1. If $A=[a_{\mu\nu}]$ $(\mu, \nu = 1 \text{ to } 3)$ and k is a scalar, write in full the matrix $A+kI_3$.

2. Find the adjoint and inverse of $\begin{bmatrix} 3 & 5 \\ 8 & 10 \end{bmatrix}$ and of $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 7 \\ 5 & 8 & 9 \end{bmatrix}$ and the adjugate and reciprocal of the corresponding determinants.

3. If $[a_1\ a_2 \dots a_n] = [b_1\ b_2 \dots b_n]M$, prove that, with the notation of p. 422, $\{a_1\ a_2 \dots a_n\} = M'\{b_1\ b_2 \dots b_n\}$.

4. If, with the notation of p. 422,

$$\{x_1\ x_2\ x_3\} = [a_{\mu\nu}]\{y_1\ y_2\ y_3\} \qquad (\mu, \nu = 1 \text{ to } 3),$$

express y_1, y_2, y_3 in terms of x_1, x_2, x_3, a_{pq}, given that $[a_{\mu\nu}]$ has rank 3.

5. Evaluate the two quotients:

$$\begin{bmatrix} 33 & 69 \\ 129 & 264 \end{bmatrix} \div \begin{bmatrix} 1 & 2 \\ 5 & 7 \end{bmatrix}$$

6. Discuss the solution of the equations

$$3x-3y+4z=2, \quad x+y+2z=-4, \quad x+4y+3z=-11,$$
$$2x+5y+5z=9.$$

7. The μ^{th} row of the matrix A is a_μ^2, a_μ, 1 and the ν^{th} column of the matrix B is 1, $-2b_\nu$, b_ν^2. If μ, ν take the values 1 to 4, use the product AB to show that $|(a_\mu - b_\nu)^2| = 0$.

8. Use the product $\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ -2b_1 & -2b_2 \\ a_1 & a_2 \end{bmatrix}$ to prove the identity

$$4(a_1c_1 - b_1^2)(a_2c_2 - b_2^2) - (a_1c_2 + a_2c_1 - 2b_1b_2)^2$$
$$= 4(a_1b_2 - a_2b_1)(b_1c_2 - b_2c_1) - (a_1c_2 - a_2c_1)^2$$

9. Show that $\begin{bmatrix} a & b & d & -c \\ b & -a & c & d \\ c & d & -b & a \\ d & -c & -a & -b \end{bmatrix}$ is orthogonal if

$a = \sin\theta \sin\phi$, $b = \sin\theta \cos\phi$, $c = \cos\theta \sin\phi$, $d = \cos\theta \cos\phi$.

10. If $[a_{\mu\nu}]$ (μ, $\nu = 1$ to n) is an orthogonal matrix, prove that $a_{p\nu}a_{q\nu} = \delta_p^q$ ($\nu = 1$ to n) where p, q take the values 1, 2, ... , n.

B

11. If the operations are possible, prove that

(i) $(A+B)' = A' + B'$ (ii) $(AB)' = B'A'$

12. If $A = \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ verify that $A^3 = A^2A = AA^2 = I_3$ and find A^{-1}.

13. Verify that $AB = BA$ when B is O, I, kI, A^n, A^{-1}.

14. If $A + I_3 = \begin{bmatrix} 1 & 3 & 4 \\ -1 & 1 & 3 \\ -2 & -3 & 1 \end{bmatrix}$ evaluate $(A + I_3)(A - I_3)$

15. If $A = \begin{bmatrix} 0 & -\tan\theta \\ \tan\theta & 0 \end{bmatrix}$ verify that

$$I_2 + A = \begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix} (I_2 - A)$$

16. If A is a square matrix, verify that $A + A'$ is symmetric ($c_{pq} = c_{qp}$) and that $A - A'$ is skew-symmetric ($c_{pq} = -c_{qp}$).

17. Use a product of matrices to prove that

$$\sum_1^4 a_r^2 \sum_1^4 b_r^2 - \left(\sum_1^4 a_r b_r\right)^2 = \Sigma(a_r b_s - a_s b_r)^2.$$

18. If the sets 1, 2, 3, 4; 1, 3, 6, 10; 1, 4, 10, 20; 1, 5, 15, x are linearly dependent, find the value of x.

Discuss the solutions of the equations in Nos. 19, 20.

19. $2x+3y+z=11t$, $4x+6y+2z=7t$, $6x+9y+4z=19t$.

20. $x+ay+a^2z=1$, $xa^{-1}+y+bz=1$, $xa^{-2}+yb^{-1}+z=1$.

21. Verify that $\frac{1}{3}\begin{bmatrix} -1 & 2 & -2 \\ -2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$ is orthogonal.

C

22. Given that $[a_{\mu\nu}]$ ($\mu, \nu = 1$ to 4) has rank 4, find the values of x_μ for which $A_{\mu\nu}x_\nu = b_\mu$

23. Use the product $\begin{bmatrix} 1 & 1 \\ \alpha & \beta \\ \alpha^2 & \beta^2 \end{bmatrix}\begin{bmatrix} x-\alpha & \alpha(x-\alpha) & \alpha^2(x-\alpha) \\ x-\beta & \beta(x-\beta) & \beta^2(x-\beta) \end{bmatrix}$

to prove that

$$\Delta \equiv \begin{vmatrix} s_0 & s_1 & s_2 & s_3 \\ s_1 & s_2 & s_3 & s_4 \\ s_2 & s_3 & s_4 & s_5 \\ 1 & x & x^2 & x^3 \end{vmatrix} = 0, \quad \text{where} \quad s_k = \alpha^k + \beta^k.$$

24. If Δ has the same meaning as in No. 23 and

$$s_k = \alpha^k + \beta^k + \gamma^k + \delta^k,$$

prove that $\Delta = \Sigma\{(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2(x-\alpha)(x-\beta)(x-\gamma)\}$.

25. If $s_k = \alpha_1^k + \alpha_2^k + \ldots + \alpha_n^k$, prove that

(i) $\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix} = \Sigma(\alpha_1 - \alpha_2)^2$

(ii) $\begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = \Sigma\{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)\}^2$.

26. If $A = [a_{\mu\nu}]$, $B = [b_{\mu\nu}]$, $C = [c_{\mu\nu}]$ ($\mu, \nu = 1$ to n), write as shortly as possible the sums of the elements of the leading diagonals of AB and ABC.

Are these sums the same for BA and BAC respectively?

27. If A, B, C, D denote the elements of matrices with r, s, r, s rows and t, t, u, u columns respectively, where $r+s=u+t$, find the ratio of $\begin{vmatrix} A & C \\ B & D \end{vmatrix}$ to $\begin{vmatrix} D & B \\ C & A \end{vmatrix}$.

28. If $a_{\mu\nu}=(\mu+\nu-1)^2$ $(\mu, \nu=1 \text{ to } n)$, prove that $|a_{\mu\nu}|=0$ if $n>4$.

29. If A is an orthogonal matrix, prove that A^{-1} is also orthogonal. State the results implied by A^{-1} being orthogonal if

$$A=[a_{\mu\nu}] \qquad (\mu, \nu=1 \text{ to } n).$$

30. If $X=AZ$, $Y=A'Z$, $A=\begin{bmatrix} 1 & c & -b \\ -c & 1 & a \\ b & -a & 1 \end{bmatrix}$, $B=A-I$,

prove that the direct transformation from X to Y is orthogonal by showing that $AA'=(I+B)(I-B)=A'A$.

31. If A is regular and $AB=AC$, prove that $B=C$.

32. If $AA'=O$ and the algebra is real, prove that $A=O$.

33. Prove that (i) if A, B are conformable, $r(A+B) \leqslant r(A)+r(B)$, (ii) if AB exists, $r(AB) \leqslant r(A)$ and $r(AB) \leqslant r(B)$.

Deduce from (ii) that if A is regular, then $r(AB)=r(B)$.

34. Verify that $[dx, dy]$ and $\left[\frac{\partial}{\partial x}, \frac{\partial}{\partial y}\right]$ are contragredient for the transformation from x, y to r, θ where $x=r\cos\theta$, $y=r\sin\theta$.

35. If $A=[a_{\mu\nu}]$ $(\mu, \nu=1 \text{ to } n)$ and $B=A-\lambda I_n$ where λ is independent of $a_{\mu\nu}$, and if $|B| \equiv b_n\lambda^n+b_{n-1}\lambda^{n-1}+\ldots+b_1\lambda+b_0=f(\lambda)$, prove that $f(A)=0$.

36. Write in determinant form the condition of collinearity of three distinct points t_1, t_2, t_3 of the rational cubic curve

$$x:y:z=a_0t^3+a_1t^2+a_2t+a_3 : b_0t^3+b_1t^2+b_2t+b_3 : c_0t^3+c_1t^2+c_2t+c_3$$

and show that it reduces to

$$\begin{vmatrix} 1 & -\Sigma t & \Sigma t_1t_2 & -t_1t_2t_3 \\ a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \\ c_0 & c_1 & c_2 & c_3 \end{vmatrix} = 0$$

CHAPTER XVIII

CHOICE AND CHANCE

Choice. Most of the principles which underlie this subject were discussed in Chapter I. We indicate here some extended applications of these principles mainly by illustrative examples. The first of these examples was solved implicitly in Chapter V, p. 100. The title of the present chapter is the same as that of a work by *W. A. Whitworth* in which the subject is treated in great detail.

Example 1. If there are n letters of the alphabet and an unlimited supply of each, find the number of ways in which a selection of r letters may be made.

If r dots and $n-1$ strokes are written down in line, each possible arrangement indicates one selection that can be made, because the strokes divide the dots into n groups (of which some may be empty groups) and the numbers in the groups may be taken as the numbers selected of the different letters. It is shown on p. 7 that the number of ways in which the dots and strokes can be arranged is $(n+r-1)!/\{(n-1)!\,r!\}$. This is therefore the number of different selections.

If the kth letter of the alphabet occurs a_k times, then

$$a_1+a_2+\ldots+a_n=r,$$

and so the number of solutions of this equation in which the a's are positive integers or zero is also $(n+r-1)!/\{(n-1)!\,r!\}$.

This is also the number of homogeneous products of r dimensions formed from n letters. See p. 100.

We add some examples of distribution problems. The number of ways in which n things can be divided into r classes depends upon whether

(i) the things are alike or different

(ii) the order of the classes is relevant or not

(iii) the order of things in a class is relevant or not

(iv) empty classes are allowed or not

(v) all the things must be distributed or not.

Example 2. Find the number of ways in which 7 different books a, b, c, d, e, f, g can be arranged

(i) in a bookcase of 4 shelves

(ii) in a bookcase of 4 shelves, none of which may be empty

(iii) in a sectional bookcase of 4 shelves or fewer, none of which may be empty

(iv) in a bookcase of 4 shelves any of which may be empty, if any of the books may first be thrown away.

(i) This is the number of ways in which 3 like strokes and the 7 different letters can be arranged in line. For example the arrangement $|bgf||ecad$ leaves the top shelf and the third empty and puts the books *bgf*, *ecad*, in that order into the second and fourth shelves.

By p. 7 the number of ways is

$$10!\div 3!, \ = 15(8!) = 604{,}800.$$

(ii) The letters can be arranged in 7! ways and from each of these arrangements a partition with no empty group is obtained by inserting dividing lines into 3 of the 6 spaces between the letters. This can be done in $\binom{6}{3}$ ways. Hence the number of arrangements of the books is

$$7!\binom{6}{3}, \ = 20(7!) = 100{,}800.$$

(iii) When there are 4 shelves the number of arrangements is $7!\binom{6}{3}$, by (ii). Similarly when there are 3, 2, 1, the numbers of arrangements are $7!\binom{6}{2}$, $7!\binom{6}{1}$, $7!$ Hence the total number is $7!(20+15+6+1)=42(7!)=211{,}680$.

(iv) If r of the 7 books are retained, they may be selected in $\binom{7}{r}$ ways; and then by the method of (i) they may be arranged in the bookcase in $(r+3)!\div 3!$ ways. Hence the number of arrangements is $\sum_1^7 \binom{7}{r}\frac{(r+3)!}{3!}$, $=1{,}203{,}328$ excluding the case in which all the books are rejected.

Note. The distinction between (i) and (iii) may be appreciated by observing that arrangements like $|\,bgf\,|\,|\,ecad$ and $bgf\,|\,ecad\,|\,|$ which put the books into different shelves in (i) become identical in (iii).

Example 3. In how many ways can the positive integer n be expressed as the sum of r positive integers not necessarily different (i) if $r=2$; (ii) if $r=3$?

Here the order of the integers is irrelevant, the partitions $a+b+c+d+e$, $c+a+e+d+b$ being regarded as identical, and zero values are excluded.

(i) If $r=2$, the number of ways is $\frac{1}{2}n$ if n is even and $\frac{1}{2}(n-1)$ if n is odd. It is therefore $[\frac{1}{2}n]$ if $[x]$ denotes the greatest integer not greater than x.

(ii) If $r=3$, suppose that the smallest integer used is k; then the other two are $k-1+x$, $k-1+y$ where x, y are positive integers such that $x+y=n-3k+2$.

Hence by (i), x and y can be chosen in $[\frac{1}{2}(n-3k+2)]$ ways. Thus the total number of ways

$$=\Sigma[\tfrac{1}{2}(n-3k+2)] \text{ for } k=1, 2, \ldots, [\tfrac{1}{3}n]$$
$$=[\tfrac{1}{2}(n-1)]+[\tfrac{1}{2}(n-4)]+[\tfrac{1}{2}(n-7)]+\ldots \text{ to } [\tfrac{1}{3}n] \text{ terms.}$$

By writing n in the form $6m+a$ for $a=0, 1, 2, 3, 4, 5$, it can be

proved that the result is the nearest integer to $\frac{1}{12}n^3$. We leave this as an exercise for the student.

The theory of *partitions*, which deals with the problem of Example 3 for a general value of r is beyond the scope of this book.

Example 4. A boy is marked for English, French, and German out of a maximum of 7 for each. In how many ways can he obtain a total of exactly 7 ? [Fractional marks are not assigned.]

Using the method of Example 18, p. 101, we see that the required number is the coefficient of x^7 in

$$(1+x+x^2+x^3+x^4+x^5+x^6+x^7)^3$$

which is the same as the coefficient of x^7 in $(1-x)^{-3}$, and this is 36.

Note. Examples 3 and 4 should be compared. In the latter, not only may zero marks be assigned, but we regard, say, $1+2+4$ as different from $2+4+1$ whereas these are reckoned as the same partition of 7. It is this kind of distinction that must be borne in mind in solving problems in our present subject.

Example 5. How many different selections of n letters can be made from $4n$ letters of which there are n a's, n b's, n c's and the others are all different ?

If the others are $d_1, d_2, \ldots, d_n$, each selection is given by the coefficient of x^n in a term of the product

$$(1+ax+a^2x^2+\ldots+a^nx^n)(1+bx+\ldots+b^nx^n)$$
$$(1+cx+\ldots+c^nx^n)(1+d_1x)\ldots(1+d_nx)$$

and therefore the *number* of selections is the coefficient of x^n in

$$(1+x+x^2+\ldots+x^n)^3(1+x)^n$$

i.e. in $(1-x^{n+1})^3(1+x)^n(1-x)^{-3}$, and this is the same as the coefficient of x^n in $\{2-(1-x)\}^n(1-x)^{-3}$, or in

$$\left\{2^n-\binom{n}{1}2^{n-1}(1-x)+\binom{n}{2}2^{n-2}(1-x)^2-\ldots+(-1)^n(1-x)^n\right\}(1-x)^{-3}$$

or in $\quad 2^n(1-x)^{-3}-n\,2^{n-1}(1-x)^{-2}+n(n-1)2^{n-3}(1-x)^{-1}$.

Therefore the required number is

$$2^{n-1}(n+1)(n+2)-n\,2^{n-1}(n+1)+n(n-1)2^{n-3}$$

which reduces to $\quad 2^{n-3}(n^2+7n+8)$.

Example 6. In how many ways can n different things be distributed amongst r men ($r<n$) so that each receives at least one thing?

We can select p_1 things for the first man in $\binom{n}{p_1}$ ways, and then select p_2 things for the second man in $\binom{n-p_1}{p_2}$ ways, and so on. Hence the number of ways in which the 1st, 2nd, ..., rth men receive $p_1, p_2, \ldots, p_r$ things where $p_1+p_2+p_3+\ldots+p_r=n$ is

$$\binom{n}{p_1}\binom{n-p_1}{p_2}\binom{n-p_1-p_2}{p_3}\ldots\binom{p_r}{p_r}, \quad \text{i.e.} \quad \frac{n!}{p_1!\,p_2!\ldots p_r!}$$

The required number of ways is the sum of expressions of this form for all possible integral values of $p_1, p_2, \ldots, p_r$, not necessarily all different, such that $p_1+p_2+\ldots+p_r=n$, and this is the coefficient of x^n in $n!\left(\frac{x}{1!}+\frac{x^2}{2!}+\ldots+\frac{x^n}{n!}\right)^r$

or in $n!(e^x-1)^r$, or in $n!\left\{e^{rx}-\binom{r}{1}e^{(r-1)x}+\binom{r}{2}e^{(r-2)x}-\ldots\right\}$.

Therefore the number of ways is

$$r^n-\binom{r}{1}(r-1)^n+\binom{r}{2}(r-2)^n-\ldots+(-1)^{r-1}\binom{r}{r-1}1^n.$$

Alternatively, by p. 2, r^n is the number of ways in which the things can be distributed if there is no stipulation that each man must receive at least one. The second term is r times the number of ways in which a particular man gets nothing and there is no other stipulation. $(r-2)^n$ is the number of ways in which two particular men get nothing; and so on. The required result can be obtained by alternate subtraction and addition. We leave the reader to verify that the number of times a particular distribution in which exactly k men ($0<k<r$) get nothing is reckoned in this process $(1-1)^k$, i.e. zero.

This problem may be compared with Exercise Ie, No. 27, (ii).

Derangements. Of the $n!$ orders in which $a_1, a_2, \ldots, a_n$ can be arranged, those in which no letter occupies its original place are called *derangements*.

Let u_r be the number of derangements of r things, and consider the $n+1$ letters $a_1, a_2, \ldots, a_n, b$. Their number (u_{n+1}) of derangements is n times the number of those in which one particular a, say a_n, comes last, because b never comes last. When a_n comes last, the other letters $a_1, a_2, \ldots, a_{n-1}, b$ must either be deranged (which implies that b is moved) or else must be arranged as a derangement of $a_1, a_2, \ldots, a_{n-1}$ followed by b (and these are mutually exclusive). There are u_n derangements of the first kind and u_{n-1} of the second; therefore there are $u_n + u_{n-1}$ derangements in which a_n is last.

Hence $$u_{n+1} = n(u_n + u_{n-1}).$$

This is a linear difference equation with variable coefficients. Its solution involves two arbitrary constants which are evaluated by observing that $u_1 = 0$, $u_2 = 1$. The equation is solved on pp. 232, 233, where it is shown that

$$u_n = n!\left\{1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\right\}$$

This value of u_n is called *sub-factorial* n and is denoted by $n\lfloor$. It may also be obtained by the alternative method suggested for Example 6.

EXERCISE XVIIIa

A

1. Find the number of ways in which $3n$ unlike things can be distributed into n groups of three.

2. In how many ways can 20 different gifts be distributed amongst 7 people any of whom may receive none?

3. In how many ways can 7 different flags be displayed on 5 distinguishable masts if all the flags and masts are used?

4. Find the number of sentences of r words that can be formed out of n different letters if each letter is used but not repeated, every arrangement of letters is regarded as a word, and every arrangement of words as a sentence.

5. A committee of n men elects its own chairman: one man, one vote. How many different forms can the result of the poll assume if the numbers of votes given to all the members are published?

6. A candidate scores $2n$ marks on four papers for each of which the maximum is n. In how many ways can this be done?

7. How many different selections of n balls can be made from b blue balls, c red balls, and d green balls, (i) if $n<b<c<d$, (ii) if $b<n<c<d$?

8. In how many ways can 15 similar oranges be distributed amongst 7 children if each must have at least one?

9. In how many ways can 12 different books be bound in green, red, and brown, if there must be at least one in each colour?

10. In how many ways can n letters be put into their n envelopes without any letter being in the right envelope, (i) if $n=3$, (ii) if $n=4$, (iii) if $n=6$?

11. n points of a plane are joined in all possible ways by straight lines, produced indefinitely both ways. If no two of these lines are parallel or coincident and no three concurrent except at the original points, prove that there are $\frac{1}{8}n(n-1)(n-2)(n-3)$ additional points of intersection.

12. Prove that, if n is a positive integer, $6n+1$ can be expressed as the sum of three positive integers (not necessarily unequal) in $n(3n+1)$ ways.

B

13. Find the number of terms of the tenth degree in a, b, c, d, e.

14. How many different arrangements of three letters can be made from the 26 letters of the alphabet if the letters must be arranged alphabetically when any of them are different?

15. In how many ways can 18 people be divided into groups of 7, 6, 5?

16. In how many ways can a lady without any thumb arrange all her 5 unlike rings on her left hand?

17. In how many ways can n men and n women sit at a round table if no two women may sit together?

18. What is the result of Example 4 if zero marks are excluded?

19. Find the number of selections of $n-3$ things that can be made from n things of which 4 are alike and the others all different?

20. Show that the number of ways in which three men each throwing a single die marked 1, 2, 3, 4, 5, 6 can obtain a total of 15 is the coefficient of x^{12} in $(1-x^6)^3(1-x)^{-3}$ and find this coefficient.

21. In how many different ways can the letters a, b, c, d, e be divided into three groups if the order of the groups and the order of the letters in each group are irrelevant and no group is empty?

22. Prove that the number of selections of n letters from the $2m$ letters $a_1, a_1, a_2, a_2, \ldots, a_m, a_m$ is the coefficient of x^n in $(1+x+x^2)^m$.

23. Find the number of selections of n letters that can be made from n A's, n B's, and n other letters all different.

24. In how many ways can I carry 12 identical coins if I have 5 pockets, and in how many of these ways will there be no empty pockets?

25. Find the number of selections of r letters that can be made from n A's, n B's n C's, when $n<r<2n+2$.

C

26. Find the number of ways in which n different books can be arranged in the r indistinguishable parts of a sectional bookcase $(n>r)$, (i) if no part may be empty, (ii) if there is no restriction.

27. Find the number of ways in which n different books can be arranged in r different shelves $(n>r)$, (i) if no shelf may be empty, (ii) if there is no restriction.

28. Prove that from $2n+1$ numbers in A.P. a set of three numbers in A.P. can be taken in n^2 ways, excluding progressions x, x, x, and reckoning x, y, z and z, y, x as the same.

29. n boys are to be arranged in a line and r of them are such that no two of them ought to be neighbours. Show that there are $(n-r)!\,(n-r+1)!/(n-2r+1)!$ suitable arrangements.

30. Through how many arbitrary points in space of three dimensions is it possible to draw a surface of order n?

31. Find the number of permutations of three letters that can be made from the $2n$ letters $a_1, a_1, a_2, a_2, \ldots, a_n, a_n$.

32. Prove that the number of permutations of m things chosen from p alike of one kind, q alike of another, etc. is the coefficient of x^m in $m!\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\ldots+\frac{x^p}{p!}\right)\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\ldots+\frac{x^q}{q!}\right)\ldots$.

33. Find the number of ways of giving $n+2$ different prizes to n boys and n girls so that each girl gets at least one.

34. Prove that $n\rfloor$ is the integer nearest to $n!\div e$.

35. Find the number of permutations of n different letters in which no letter is more than one place away from its original position.

36. Two coplanar pencils are composed of p and q lines of which no two are parallel and of which the line joining the vertices is not one. Show that the plane is divided into $pq+2p+2q-1$ parts.

37. Prove that the number of different triangles that can be formed from n straight rods of lengths 1, 2, 3, ..., n units is $\frac{1}{24}n(n-2)(2n-5)$ if n is even, and $\frac{1}{24}(n-3)(n-1)(2n-1)$ if n is odd.

Probability. The importance and some of the interest of this subject are due to the part it plays in the theory of statistics. This theory, besides having many industrial and technical applications, is now used in such subjects as physics and biology.

These applications lie outside the scope of this work. The reader who is interested may refer to

(i) A First Course in Statistics : D. C. Jones,

(ii) An Introduction to Mathematical Probability : J. L. Coolidge,

(iii) Mathematical Theory of Probabilities : Arne Fisher,

(iv) Probability and its Engineering Uses : T. C. Fry.

In the following pages we give little more than a collection of examples to show what meaning is attached to the word '*chance*' in mathematical language.

If a bag contains 8 balls which are all alike except that 3 are red and 5 blue, and if a ball is drawn 'at random' from the bag, the *probability* or *chance* that a red ball will be drawn is said to be $\frac{3}{8}$ and that a blue ball will be drawn is said to be $\frac{5}{8}$. Also the odds are said to be 5 : 3 in favour of blue.

The term *chance* is used in ordinary language in much more complicated examples than that just given, and in many of these

it is difficult or impossible to assign a definite numerical value to the chance.

Even in the examples which are susceptible of numerical treatment the chance is reckoned *relative to some particular body of knowledge* stated or implied.

For example, consider the statement:

'January 1st, 2501 will be a Sunday unless the Gregorian calendar is abandoned.'

To a man who only knows that January 1st will be one of the seven days of the week, the chance that the statement is true is $\frac{1}{7}$. But to one who has made the necessary calculation (or happens to know that a century never begins on a Sunday) there is no chance that the statement is correct.

The chance of an impossible event is said to be 0, and the chance of an event that is certain to take place is said to be 1.

Chances of doubtful events are measured by numbers between 0 and 1 and are assigned so that if there are two or more events of which only one can take place, *the sum of their chances is equal to the chance that one or other of them will take place.* In particular this sum is 1 if it is certain that one or other of the events must happen.

The ideas implied by the phrases 'equally likely' and choosing 'at random' are taken for granted.

When a coin is tossed it is assumed to be 'equally likely' to turn up head or tail. This is interpreted to mean that the chances of head and tail are equal. Since either head or tail must turn up, the sum of the chances is taken to be 1. Hence the chance of head is $\frac{1}{2}$ and the chance of tail is $\frac{1}{2}$.

Again in the illustration on p. 462, when one of the 8 balls is drawn out 'at random', each ball's chance is $\frac{1}{8}$. The chance that a red ball is drawn is the sum of the chances of the separate red balls, namely $\frac{1}{8}+\frac{1}{8}+\frac{1}{8}$, and the chance that a blue ball is drawn is $\frac{5}{8}$. The sum of these chances $\frac{3}{8}$ and $\frac{5}{8}$ is 1, it being certain that either a red or a blue ball will be drawn.

The validity of the idea of random choice becomes doubtful when there is an unlimited choice. The questions

"If a natural number is selected at random, what is the chance that it is (i) less than 1000, (ii) prime?"

might be interpreted as

$$\text{Find the values of (i) } \lim_{n\to\infty} \frac{999}{n}, \quad \text{(ii) } \lim_{n\to\infty} \frac{\pi(n)}{n}$$

where $\pi(n)$ is the number of prime numbers less than n. If so, the answers are both zero. But in fact when people are asked to choose numbers at random they often choose numbers less than 1000 or prime numbers. These paradoxes may be explained by the natural prejudice against choosing numbers that are so large that it would take a lifetime to pronounce their names. In fact we cannot choose a number at random.

On the other hand if ABC is a straight line and $AB = 2BC$ it seems reasonable to assume that we can choose a point P at random in AC and to take the chances that P lies within AB, BC to be $\frac{2}{3}$, $\frac{1}{3}$ respectively, although this implies that the chance that P coincides with B is zero. See also Exercise XVIIIb, No. 24.

Chances are sometimes affected by non-mathematical considerations. For example it is found that people asked to choose a number less than 10 have an undue preference for 7. And when a coin is tossed there is some chance that the toss will miscarry; if this chance is ϵ, the chances of head and tail are each $\frac{1}{2}(1-\epsilon)$.

Independent Events. Two events are called *independent* if the probability that either happens is unaffected when the other event happens or fails to happen.

Example 7. A bag contains 2 red balls and 1 blue ball (R_1, R_2, B_1) and a second bag contains 4 red balls and 3 blue balls (r_1, r_2, r_3, r_4, b_1, b_2, b_3). A ball is drawn at random from the first bag and another is drawn at random from the second. What is the chance that these balls will be both red?

The two events are independent; that is the colour of the ball drawn from the first bag does not affect the chance that a red ball will be drawn from the second bag.

It is easy to enumerate all the different possible draws: R_1r_1, R_1r_2, ..., B_1b_3. Their number is 3×7 and in 2×4 of these draws both balls are red. Since all the draws are equally likely, the required chance is $\frac{2 \times 4}{3 \times 7} = \frac{8}{21}$.

Now the chance that a red ball will be drawn from the first bag is $\frac{2}{3}$ and from the second bag $\frac{4}{7}$; hence the enumerative method shows that the chance that both will be red is the product of the chances of the two independent events.

More generally **if the chances of two independent events are p, p', the chance that both will take place is pp'.** For suppose that the first can happen in a ways and fail in b ways, all these ways being equally likely; then $p = a/(a+b)$. Similarly suppose that the second can happen in c ways and fail in d ways, all equally likely; then $p' = c/(c+d)$. Out of the $(a+b)(c+d)$ possibilities there are ac in which both events happen. Hence the chance that both events happen is $ac \div \{(a+b)(c+d)\}$ which equals pp'.

It follows that if p, p' are the probabilities of independent events A and B, then

$$pp' \qquad p(1-p') \qquad (1-p)p' \qquad (1-p)(1-p')$$

are the probabilities of the compound events

A and B $\quad$ A but not B $\quad$ B but not A $\quad$ neither A nor B.

No interpretation can be given to the chance $p+p'$ in this case of independent events. But since the compound events 'neither A nor B' and 'at least one of A, B' are such that one or other must happen, it follows that $1-(1-p)(1-p')$ is the probability that at least one of the two events A and B will occur.

The formula pp' for the probability of a compound event 'A and B' where A, B are independent, is sometimes used when the proof that has been given is not applicable.

For instance if two points P, Q are chosen independently in the line ABC, where $AB=2BC$, the chance that both points should be in AB would be taken to be $\frac{2}{3}\times\frac{2}{3}$.

The chance $(a\div N)$ of an event is often found as in Example 7 by a direct appeal to the definition. It is the ratio of the number of different ways (a) in which the event can take place to the total number (N) of equally likely possibilities. In such cases the problem is solved by methods that have already been discussed under the heading of 'Choice', as in some of the following examples.

Example 8. Find the chance of throwing at least one ace in a single throw of two dice.

First Method. Each die can fall in 6 ways; therefore there are 36 possible throws. The cases in which an ace occurs are: 1, 1; 1, 2; 1, 3; 1, 4; 1, 5; 1, 6; 2, 1; 3, 1; 4, 1; 5, 1; 6, 1; and are 11 in number. Hence the chance is $\frac{11}{36}$.

Second Method. The chance of not throwing an ace is $\frac{5}{6}$ for the first die and $\frac{5}{6}$ for the second; therefore the chance of not throwing an ace with either is $\frac{25}{36}$. Hence the required chance is $1-\frac{25}{36}$, $=\frac{11}{36}$.

Example 9. What is the least number of dice that must be thrown so that it is more likely than not that at least one six will fall?

As in Example 8, if n dice are thrown, the chance that no six falls is $(\frac{5}{6})^n$. Hence n must be chosen so that

$$(\tfrac{5}{6})^n<\tfrac{1}{2} \qquad \therefore\ n\log\tfrac{5}{6}<\log\tfrac{1}{2}$$

$$\therefore\ n>\frac{\log 2}{\log 1\cdot 2}\simeq 3\cdot 8$$

Hence the least value of n is 4.

Example 10. Find the chance of throwing a total of exactly 15 with four dice.

It was shown in Example 18, p. 101, that the number of ways of throwing 15 is the coefficient of x^{15} in $(x+x^2+x^3+x^4+x^5+x^6)^4$ and that this coefficient is 140. See also Example 4, p. 457.

But the number of possible throws is 6^4. Hence the chance is $\frac{140}{6^4}, = \frac{35}{324}$.

Example 11. A car meets with an accident on an average once in 4 years. What is the chance that 12 years elapse without an accident?

Since there is an unlimited number of instants at which the accident may happen, this is an example to which the remarks on p. 464 are applicable.

Let the 4-year period be divided into k equal intervals. Assume that the event can happen just once in an interval and that the chance that it does so in any one particular interval is $1/k$. Then the chance that it does not happen in the $3k$ intervals is $\left(1-\frac{1}{k}\right)^{3k}$. But when k increases indefinitely $\left(1-\frac{1}{k}\right)^{3k} \to e^{-3}$. Hence the chance that the car will be free from accidents for 12 years is taken to be e^{-3} ($\simeq \frac{1}{20}$).

Similarly the probability that no accident will occur in any assigned period of 4 years is e^{-1} ($\simeq \cdot 37$). Thus the chance of escaping an accident in the 4 years is less than $\frac{1}{2}$.

Example 12. Find the chance of throwing exactly r heads in n tosses of a coin.

Out of the 2^n possible results of n tosses, there are $\binom{n}{r}$ in which there are exactly r heads. Hence the chance is $\binom{n}{r} \Big/ 2^n$.

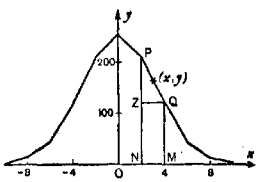
This is the $(r+1)^{\text{th}}$ term of the binomial expansion of $(\frac{1}{2}+\frac{1}{2})^n$.

If a large number of tosses is made, we expect to get about as many heads as tails. If the number is $2N$, the chance of getting N heads and N tails is $(2N)!/(N!\,2^N)^2$. This is larger than the chance of getting any other particular distribution, say $N+k$ heads and $N-k$ tails, though not so large as the chance that the numbers of heads and tails will differ by 2. (See also Exercise XVIIIc, No. 12.)

It is interesting to represent graphically the probabilities of different distributions. If p is the probability that there are x more heads than tails in n tosses, the result of Example 12 shows that

$$y \equiv 2^n p = \binom{n}{\frac{1}{2}n + \frac{1}{2}x}$$

For $n = 10$, the values of y corresponding to $x = 0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10$ are 252, 210, 120, 45, 10, 1 respectively and these are represented in the diagram.



This is called a *frequency polygon* because it shows the frequency with which the different distributions are to be expected in a large number of trials. In this example x can only take even integral values. In a problem involving a continuous variable, which implies an infinity of values of x, the frequency polygon is replaced by a *frequency curve* $y = f(x)$ such that the number of values to be found in the interval $x, x + \delta x$ is $f(x)\delta x$. The form of the function $f(x)$ in a case of normal distribution may be conjectured from the above example. If (x, y) is the middle point of the side PQ of the polygon joining the points given by $x = 2k, 2k + 2$

$$-\frac{1}{y}\frac{dy}{dx} = \frac{2}{PN + QM}\frac{PZ}{ZQ} = \frac{PN - QM}{PN + QM}$$

and

$$\frac{QM}{PN} = \binom{n}{\frac{1}{2}n + k + 1} \div \binom{n}{\frac{1}{2}n + k} = \frac{\frac{1}{2}n - k}{\frac{1}{2}n + k + 1}$$

$$\therefore \quad -\frac{1}{y}\frac{dy}{dx} = \frac{2k+1}{n+1} = \frac{x}{n+1}$$

Integration gives

$$y = ae^{-\frac{x^2}{2(n+1)}}$$

where a is the value of y for $x = 0$.

This equation represents a curve which touches the sides of the polygon at their middle points. The curve is called the *error*

curve or the *normal curve of frequency of error* because it is found by experience that many variations of ordinary quantities, such as errors of observation, are distributed in the way indicated by this curve. Its properties and use are discussed in books on statistics, and an interesting elementary account is given in Nunn's Algebra, Part II, pp. 440-486.

Compound Events and Dependent Events. In the compound events such as 'A and B', 'A but not B', considered on p. 465, A and B are independent events. In the following example we are concerned with a pair of events A, B such that the probability of B depends upon whether A takes place or not.

Example 13. One ball was drawn at random from a bag containing 5 white and 3 black balls; 1 white and 1 black ball were then placed in the bag. Find the chance that a ball now to be drawn at random from the bag will be white.

[The chance depends upon the result of the first draw. To a man who knows that a black ball was drawn, the chance is $\frac{6}{9}$ because he knows that there are now 6 white and 3 black balls in the bag; and if he knows that the ball drawn was white, the chance *to him* is $\frac{5}{9}$. But we are to calculate the chance to a person who does not know the result of the first draw.]

The chance that a white ball will be drawn is the sum of the chances that the draws are 'white then white' and 'black then white', because only one of these compound events can take place. For the first of these compound events to take place a white ball must be drawn from 5 white and 3 black and then independently a white ball must be drawn from 5 white and 4 black. Thus the chance is $\frac{5}{8} \times \frac{5}{9}$. Similarly the chance of the second compound event is $\frac{3}{8} \times \frac{6}{9}$. Hence

$$\text{the required chance} = \tfrac{5}{8}\ \tfrac{5}{9} + \tfrac{3}{8}\ \tfrac{6}{9} = \tfrac{43}{72}.$$

The next example shows that the chance in Example 13 would be different if the addition of the white and black balls had been made *before* the first ball was drawn.

Example 14. One ball was drawn at random from a bag containing 6 white and 4 black balls. Find the chance that a ball now to be drawn at random from the bag will be white.

For the first ball the chances were: white $\frac{3}{5}$, black $\frac{2}{5}$.

For the second ball to be white, the chance is now $\frac{5}{9}$ or $\frac{6}{9}$.

Hence as in Example 13 the required chance $= \frac{3}{5}\cdot\frac{5}{9} + \frac{2}{5}\cdot\frac{6}{9} = \frac{3}{5}$

The result of Example 14 shows that the chance of drawing a white ball is the same for the second draw as for the first. More generally if balls are drawn continually from a bag containing p white and q black balls, the chance of drawing white at the n^{th} draw is always $p/(p+q)$ for $1 \leqslant n \leqslant p+q$; for in the $(p+q)!$ possible orders in which the balls may be drawn, there are $(p+q-1)! \times p$ in which the n^{th} ball is white.

The method used in the above examples may be generalised to show that if the probability of B is x when A has occurred and y when A has failed to occur, and if the probability of A is p, then the probability of B is $px + (1-p)y$.

Example 15. A bag contains four balls each of which is either black or white. Find on each of the following different hypotheses the chance that two balls drawn at random from the bag will be one black and one white:

(i) each ball is equally likely to be black or white,

(ii) the distributions 4 black, 3 black and 1 white, 2 black and 2 white, 1 black and 3 white, 4 white, are all equally likely,

(iii) one ball is black, one is white, and each of the others is equally likely to be black or white.

(i) By the argument on p. 467 it follows that the chances of the five distributions are $\frac{1}{16}$, $\frac{4}{16}$, $\frac{6}{16}$, $\frac{4}{16}$, $\frac{1}{16}$ and the corresponding chances of drawing one black and one white are $0, \frac{3}{6}, \frac{4}{6}, \frac{3}{6}, 0$. Hence the chance $= 0 + \frac{4}{16}\cdot\frac{3}{6} + \frac{6}{16}\cdot\frac{4}{6} + \frac{4}{16}\cdot\frac{3}{6} + 0 = \frac{1}{2}$

(ii) The chance of each of the five distributions is $\frac{1}{5}$ and the required chance $= \frac{1}{5}(\frac{3}{6} + \frac{4}{6} + \frac{3}{6}) = \frac{1}{2}$

(iii) The distribution must be 3 black and 1 white, 2 black and 2 white, or 1 black and 3 white and the chances of these are $\frac{1}{4}, \frac{1}{4}, \frac{1}{4}$. Hence the required chance $= \frac{1}{4} \cdot \frac{3}{8} + \frac{1}{4} \cdot \frac{4}{8} + \frac{1}{4} \cdot \frac{5}{8} = \frac{1}{16}$.

Expectation. If there is a chance p that a man will win a prize worth £M, then £pM is called the value of his *expectation*. It is regarded as the fair price for him to pay to obtain the chance of winning the prize. This is based on the assumption that if he paid this price on a large number (n) of occasions, he might expect to win the prize pn times and thus to recover his outlay.

Example 16. A man throws a pair of dice and is to receive £2^{1-n} if the first occasion on which an ace appears is at the n^{th} throw. What is the value of his expectation?

By Example 8, p. 466, the chance of throwing an ace is $\frac{11}{36}$. Hence the chance that the ace first appears at the r^{th} throw is $(\frac{25}{36})^{r-1}\frac{11}{36}$ and the value of the expectation is

$$\lim_{n\to\infty} \sum_{r=1}^{n} \{(\tfrac{25}{36})^{r-1}\tfrac{11}{36}2^{1-r}\} \text{ pounds}.$$ The limit is $\frac{11}{36}/(1-\frac{25}{72})$, or $\frac{22}{47}$.

Thus the value of his expectation is about 9s 4d.

Example 17. (The Petersburg Paradox.) B tosses a coin. C promises to pay to B 1, 2, 4, 8, ... florins according as head first appears at the 1st, 2nd, 3rd, 4th, ... toss. What is the fair price for B to pay to C for this promise?

The chance that head first appears at the nth toss is 2^{-n}; and if it does, B receives 2^{n-1} florins. Hence B's expectation of gain by the appearance of the first head at the n^{th} toss is one shilling. This is true for $n = 1, 2, 3, \ldots$ and therefore B's total expectation appears to be unlimited.

It is argued that few people would be willing to pay even such a sum as £5 for the promise. The problem assumes that C's wealth is unlimited. If he only possesses £10^6, B's expectation is reduced to about 25 shillings. B should also consider whether he can afford to invest even 25 shillings sufficiently often to get the run of tails necessary to restore his fortune.

Inverse Probability. When an event has taken place and it is known that its occurrence was due to one of several mutually exclusive causes, the calculation of the probabilities of those causes or of other events due to them is called a problem of *inverse probability*. Such a problem can only be solved by making certain assumptions, and these are illustrated in Examples 18, 19, 20.

Example 18. (i) One bag contained 8 sovereigns and 16 worthless counterfeits and a second bag contained 18 sovereigns and 6 worthless counterfeits. One of the bags was selected at random and a coin was drawn at random from it. Find the chance that this coin was a sovereign.

(ii) On a certain occasion the coin so drawn was found to be a sovereign. What then would be a fair price to pay for the coins remaining in the selected bag?

(i) The chance of selecting the first bag and drawing a sovereign from it is $\frac{1}{2} \times \frac{8}{24}$ and the chance of selecting the second bag and drawing a sovereign from it is $\frac{1}{2} \times \frac{18}{24}$. Hence the chance of drawing a sovereign $= \frac{4}{24} + \frac{9}{24} = \frac{13}{24}$.

(ii) Suppose that the experiment in (i) is repeated a large number of times, say $24N$. Now assume that the results will be as follows: In $12N$ experiments the first bag is selected; in $4N$ of these a sovereign is drawn, in the other cases a counterfeit. In the other $12N$ experiments the second bag is selected; in $9N$ of these a sovereign is drawn, in the other cases a counterfeit.

Considering only the $13N$ experiments in which a sovereign is drawn, there are $4N$ of them in which it was drawn from the first bag and $9N$ from the second. The total value of the remaining coins in the selected bag in these $13N$ cases is $£(4N.7 + 9N.17)$, i.e. $£(181N)$. Hence $£(181N \div 13N)$ is a fair price to pay on each occasion. This is approximately £13 18s 6d. It is customary to obtain this result more shortly as follows. (See also Example 19.)

The chance of drawing a sovereign is $\frac{1}{2}$ if the first bag is selected and $\frac{3}{4}$ if the second is selected. Hence the principle of inverse probability states that when a sovereign has been observed to be drawn the chances that the selected bag was the first or second are in the ratio $\frac{1}{2} : \frac{3}{4}$, i.e. 4 : 9 and are therefore $\frac{4}{13}, \frac{9}{13}$. Hence the fair price $= £(\frac{4}{13}\,7 + \frac{9}{13}\,17) = £13\frac{1}{13}$, as before.

The theory of errors shows that the probable error in such a statement as that in $24N$ experiments the first bag is selected $12N$ times is of the order $k\sqrt{N}$ where k is independent of N, and the other assumptions are subject to similar probable errors. Since $(\sqrt{N}) \div N \to 0$ when $N \to \infty$, the result obtained above is correct if it may be supposed that N increases without limit.

Example 19. A bag contains four balls each of which is either black or white. Two balls are drawn from it, are found to be one black and one white, and are replaced. Find the chances that two balls afterwards drawn at random will be one black and one white assuming (i) that originally each ball is equally likely to be black or white, (ii) that originally one ball is known to be black, one is known to be white and the others are equally likely to be black or white.

(i) After the first draw one ball is known to be black and one to be white. Hence the problem is equivalent to Example 15 (iii).

The original chances of the five distributions are

$4B$	$3B, 1W$	$2B, 2W$	$1B, 3W$	$4W$
$\frac{1}{16}$	$\frac{4}{16}$	$\frac{6}{16}$	$\frac{4}{16}$	$\frac{1}{16}$

and the chances of drawing one black and one white are then

$$0 \qquad \tfrac{1}{2} \qquad \tfrac{1}{2} \qquad \tfrac{3}{8} \qquad 0$$

and therefore the chances of the compound events are

$$0 \qquad \tfrac{4}{16}\,\tfrac{1}{2} \qquad \tfrac{6}{16}\,\tfrac{1}{2} \qquad \tfrac{4}{16}\,\tfrac{3}{8} \qquad 0$$

By the principle of inverse probability the chances that the bag contained the 2nd, 3rd, 4th distributions are as 1 : 2 : 1 and are therefore $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$. Hence the required chance

$$= \tfrac{1}{4}\,\tfrac{3}{8} + \tfrac{1}{2}\,\tfrac{4}{8} + \tfrac{1}{4}\,\tfrac{3}{8} = \tfrac{7}{11}$$

(ii) The chances of the three possible distributions are

$$\begin{array}{ccc} 3B, 1W & 2B, 2W & 1B, 3W \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \end{array}$$

and the chances of drawing one black and one white are then

$$\frac{3}{6} \qquad \frac{4}{6} \qquad \frac{3}{6}$$

and therefore the chances of the compound events are

$$\frac{1}{4}\,\frac{3}{6} \qquad \frac{1}{2}\,\frac{4}{6} \qquad \frac{1}{4}\,\frac{3}{6}$$

By the principle of inverse probability the chances that the bag contained the 1st, 2nd, 3rd distributions are as $3 : 8 : 3$ and are therefore $\frac{3}{14}$, $\frac{8}{14}$, $\frac{3}{14}$. Hence the required chance

$$= \tfrac{3}{14}\,\tfrac{3}{6} + \tfrac{8}{14}\,\tfrac{4}{6} + \tfrac{3}{14}\,\tfrac{3}{6} = \tfrac{25}{42}$$

EXERCISE XVIIIb

A

1. A coin is tossed five times. What is the chance of (i) five heads, (ii) at least three heads ?

2. Four dice are thrown. What is the chance of getting two or more sixes ?

3. If the chances that three independent events E_1, E_2, E_3 occur are p_1, p_2, p_3, find the chance that (i) E_1 and E_2 occur and E_3 does not, (ii) E_2 occurs and E_1, E_3 do not.

4. If the chance that any particular day in July will be fine is $\frac{3}{4}$, find the chance that all seven days of the first week in July will be fine.

5. A man applied for three jobs and his chances of getting them were $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$. What is the chance that he gets at least one ?

6. m different odd numbers and n different even numbers are written down at random, where $m \leqslant n+1$. Show that the chance that no two odd numbers are adjacent to one another is

$$n!(n+1)!/\{(m+n)!(n-m+1)!\}$$

7. Twelve balls are selected at random from an unlimited number of red, green, and blue balls. Find the chance that there is at least one of each colour.

8. One bag contained 8 red and 4 white counters, and another bag contained 2 red and 3 white. From one of these bags selected at random a counter was drawn at random and found to be red. If a red counter is worth 5s and a white one 2s, what is a fair price to pay for the counters remaining in the selected bag?

9. What is the fallacy in the following argument?

A point is chosen at random in a line. Divide the line into n equal parts. The chance that the point is not in the first part is $1 - 1/n$. Similarly for the other parts. Hence the chance that it is in no part at all is $(1 - 1/n)^n$, i.e. about e^{-1} if n is large.

10. One bag contains b red tickets and c white tickets; another contains c red and b white tickets. One ticket is drawn at random from each bag and (after both are drawn) put into the other bag. If a red ticket is worth one shilling and a white one is worthless, how many shillings would you give for the contents of the first bag after the operation?

11. A bag contained 4 balls, each of which was either blue or red but they were not all of one colour, and the distributions $1B + 3R$, $2B + 2R$, $3B + 1R$ were equally likely. Two balls were afterwards drawn at random from the bag and found to be one of each colour. If these are now replaced in the bag and two balls are again drawn at random, what is the chance that these will be one blue and one red?

12. A man put five coins into a purse, deciding at random for each coin separately whether it was to be a sovereign or a shilling. Two coins were then drawn at random from the purse and were found to be sovereigns. They were then replaced. What is now a fair price to pay for the contents of the purse?

13. If in No. 12, instead of two coins being drawn, one was drawn and found to be a sovereign and was replaced, and then again one was drawn, found to be a sovereign and replaced, what is now the fair price?

B

14. A coin is tossed three times. What is the chance of three tails?

15. What are the chances of winning (i) exactly 5, (ii) 5 or more tosses out of 10?

16. What is the chance of getting a total of exactly 21 in one throw of six dice?

17. n persons are seated at a round table. $n > 3$. If 3 of them are chosen at random, what is the chance that at least 2 of these are neighbours?

18. One bag contains mp white and $m(1-p)$ black balls and another bag contains nq white and $n(1-q)$ black balls. One of these bags is chosen at random and a ball is drawn from it at random. Find the chance that this ball will be black.

Also find the conditions that this chance is (i) equal to, (ii) greater than, the chance of drawing a black ball from a bag containing all the $m+n$ balls.

19. From a bag of 9 black and 9 white balls, 9 are drawn at random one at a time, the ball drawn being immediately replaced after each draw. Show that the chance that 4 of each kind will be drawn is a little less than $\frac{1}{2}$.

20. A bag contained 5 balls each black or white and equally likely to be either. A ball was then drawn from the bag and found to be black. What is now the chance that the bag originally contained 2 black and 3 white balls?

21. There were five coins in a purse, equally likely to be: 5 sovereigns; 4 sovereigns and 1 shilling; 3 and 2; 2 and 3; 1 and 4; or 5 shillings. Two coins were then drawn at random from the purse and found to be sovereigns. What is now a fair price to pay for the contents of the purse?

C

22. In an ordinary deal of 52 cards to four players, find, approximately, the chance that the dealer receives the whole of one suit. [If n is large $n! \simeq (n/e)^n \sqrt{(2\pi n)}$.]

23. A coin is tossed $p+q$ times. $p>q$. Prove that the chance of at least p consecutive heads appearing is $(q+2)/2^{p+1}$.

24. Find the chances that a random chord of a circle is longer than the radius on the following assumptions:

(i) all distances from the centre are equally likely,

(ii) all angles subtended by the chord at the centre are equally likely,

(iii) all lengths are equally likely.

25. If 7% of the population escapes getting a cold during any given year, how many days must the average inhabitant expect to wait from one cold to the next?

26. If integers m, n are chosen at random, what is the chance that m^2+n^2 is divisible by 5?

27. Three tickets are drawn at random from a set of $6n$ tickets numbered from 0 to $6n-1$. Show that the chance that the sum of the numbers on the tickets drawn is $6n$ is $3n/\{(6n-1)(6n-2)\}$

MISCELLANEOUS EXAMPLES

EXERCISE XVIIIc

A

1. Out of n balls of which p are white and the rest are all different colours, in how many ways can a selection of one or more be made ?

2. In how many ways can a party of 9 be divided between two cars holding 5 and 4 if only three of them can drive ?

3. In how many ways can one get rid of 6 different presents if there are 4 people to whom they may be given, and to what is this number reduced if each must have at least one present ?

4. A bag contains 5 white and 7 black balls. What is the chance that if 2 balls are drawn at random from it, they will both be white ?

5. A pair of positive integers is chosen so that their sum is 75. If all pairs are equally likely, find the chance that their product is greater than 1100.

6. The chances that 5 particular candidates will pass an examination are p, q, r, s, t. Find the chance that 3 will pass and 2 fail.

7. A pack of 52 cards is dealt to 4 players. One of them has 6 spades. What is the chance that his partner has the other 7 ?

8. What is the chance of throwing exactly 8 at least once in n throws with two dice ?

9. A tosses three shillings and B tosses two. Find the chance that A gets more heads than B.

10. A man tosses a coin repeatedly and scores 1 for each head and 2 for each tail. Find the chance p_n that his score will ever be n, by first proving that $2p_n = p_{n-1} + p_{n-2}$.

11. A bag contained four balls of which one was black, one was white, and each of the others was either black or white and equally likely to be either. Two balls were then drawn at random from it and found to be one black and the other white, and were replaced. Afterwards two balls were drawn again with the same result and were replaced. Find the chance that it will happen a third time.

12. A coin is tossed $2n$ times. Prove that if n is large, the chance that there are exactly n heads is about $1/\sqrt{(n\pi)}$. See Exercise XVIIIb, No. 22.

B

13. In how many ways can a form of 14 boys be classified as α, β, γ, δ ?

14. From p purple tickets, q green tickets, r red tickets, in how many ways can a selection of one or more be made ?

15. In how many ways can a candidate obtain $3n+1$ marks out of $4n$ for three papers with maxima n, n, $2n$?

16. How many groups of exactly n balls can be formed out of a, b, c, d balls of four different colours, if $a<n<b<c<d$?

17. How many times must a man be allowed to toss a coin in order that the chance he gets at least one head is not less than $\frac{9}{10}$?

18. Each of p points in a line AB is joined to each of q points in a line AC by an unproduced line. Prove that excluding the $p+q$ points, the joining lines meet in $\frac{1}{4}pq(p-1)(q-1)$ points.

19. In how many ways can the 10 letters from A to J be arranged so that A is not first and J is not last ?

20. A bag contains 3 red, 5 yellow, and 8 blue balls. If three balls are drawn at random from it, show that the chance that they are of different colours is $\frac{8}{14}$.

21. A bag contained four balls each of which was black or white, and was equally likely to be either. Two balls were afterwards drawn from it at random and found to be white, and were replaced. If two balls are again drawn at random, find the chance that one will be black and the other white.

22. If n people each write down at random one of the first n integers, find the chance that the first r integers ($r<n$) will not all be written, and show that the chance that all n will be written is $n!\, n^{-n}$.

C

23. If $2n$ different things are divided into pairs, prove that the chance that 3 given things are none of them paired is

$$(2n-4)/(2n-1).$$

24. If n is the sum of p positive integers the greatest of which is q, prove that it can also be expressed as the sum of q positive integers the greatest of which is p.

25. n different things are distributed at random amongst x men and y women. Find the chance that the total number received by the men is an odd number.

26. If n is a positive integer, prove that $6n+3$ can be expressed as the sum of 3 positive integers not necessarily unequal in $3n^2+3n+1$ ways.

27. Prove that n lines of which no two are parallel and no three concurrent divide a plane into $\frac{1}{2}(n^2+n+2)$ regions.

28. A bag contained n balls each of which was black or white and the chances of the $n+1$ possible distributions of black and white were equal. A ball was then drawn at random and found to be white. It was replaced, and again a ball was drawn at random, found to be white and replaced. Find the chance that a ball now drawn at random will be black.

29. There are two candidates, National and Communist, for a constituency of $m+n$ voters. The electors are such that the chance that any particular one will vote is p. Also m of them will vote National if they vote at all and n of them will vote Communist if they vote at all. Prove that the chance of a tie is the coefficient of x^m in the expansion of

$$\{p+(1-p)x\}^m\{(1-p)+px\}^n.$$

30. A and B possess a and b counters respectively. They toss coins, the loser always giving the winner a counter. If A's chance of winning all B's counters is $f(a, b)$, prove that

$$2f(a, b)=f(a+1, b-1)+f(a-1, b+1),$$

and hence evaluate the chance.

31. It takes 5 minutes to cross a certain bridge and 1000 people cross it in a day of 12 hours, all times of day being equally likely. Find approximately the chance that there will be nobody on the bridge at noon.

32. On a line AB two points P, Q are taken at random in the order $APQB$. Prove that the chance that a triangle can be drawn with sides equal to AP, PQ, QB is $\frac{1}{4}$.

33. A pack of 52 cards is laid face downwards. A person names a card, and then this card and all above it are handed to him; he then names another card and the same process is repeated and this is continued until none are left. Find the chance that during the process he names the top card at least once.

34. Each of two boxes P and Q contains one black and one white ball. A ball chosen at random from P is placed in Q, and then a ball chosen at random from Q is placed in P. This process is repeated continually. Find the chance that after n double transferences, the balls in P are for the first time both white.

CHAPTER XIX

THEORY OF NUMBERS

THE positive or the signless integers *excluding unity* can be divided into two classes: *composite numbers* which can be expressed as the product of two smaller integers, and *prime numbers* which cannot be so expressed. Thus the series of primes begins with 2, 3, 5, 7, 11, 13, 17, ...

The theory of numbers deals mainly with properties of numbers arising out of this classification, and for the most part it involves analysis far beyond the scope of this book. But in contrast with most branches of mathematics many of its enquiries can be expressed in language intelligible to the non-specialist.

The number of primes is unlimited. For if x is the product of any given set of primes, $1+x$ is either prime or else is divisible by a prime that does not belong to the set; in either case a prime exists not belonging to the set.

On the other hand the answers to the following problems, in spite of their apparent simplicity, are as yet unknown:

Is there at least one prime between n^2 and $(n+1)^2$ for all positive integral values of n?

Is there an unlimited number of primes of the form n^2+1?

Is there an unlimited number of pairs of primes (like 17, 19) of the form $2n-1$, $2n+1$?

Can an even number greater than 2 always be expressed as the sum of two primes? This is known as *Goldbach's problem*; it has been proved that any integer (greater than 3) can be expressed as the sum of not more than κ primes where κ is a constant independent of n.

Distribution of Primes. Prime numbers may be found by the *Sieve of Eratosthenes* as follows: write down the integers 2, 3, 4, 5, 6, 7, 8, ... as far as may be required; strike out all the multiples of 2, then all the multiples of 3, then all the multiples of the next number that has not been struck out (5), and so on. The numbers that would never be struck out are prime. By the time the multiples of, say, 11 have been struck out, the list of primes will be complete up to 167, because every composite number less than 13^2 must have a prime factor less than 13.

The number of primes less than or equal to a number x is denoted by $\pi(x)$. No exact formula has been discovered for $\pi(x)$, but it has been shown that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

This is called the *prime number theorem*; the proof is too difficult for inclusion here. Also a good approximation for $\pi(x)$ when x is large is given by the logarithmic integral $\operatorname{li} x$ which is defined as

$$\lim_{\epsilon\to 0+} \left\{ \int_0^{1-\epsilon} \frac{dt}{\log t} + \int_{1+\epsilon}^{x} \frac{dt}{\log t} \right\}.$$

For example $\pi(x)/\operatorname{li} x$ is approximately ·94 when $x = 1000$ and approximately ·998 when $x = 1000000$. (See *The Distribution of Prime Numbers*: A. E. Ingham.)

Again no formula can be given for the n^{th} prime number p_n, but it can be deduced from the prime number theorem that

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1$$

For since $\pi(p_n) = n$, the theorem gives $\lim \dfrac{n \log p_n}{p_n} = 1$, hence

$$\lim (\log n + \log\log p_n - \log p_n) = 0,$$

and
$$\lim \frac{\log n + \log\log p_n - \log p_n}{\log p_n} = 0;$$

but
$$\lim \frac{\log\log p_n}{\log p_n} = 0, \quad \text{thus} \quad \lim \frac{\log n}{\log p_n} = 1$$

and
$$\lim \frac{n \log n}{p_n} = \lim \frac{\log n}{\log p_n} . \lim \frac{n \log p_n}{p_n} = 1.$$

Although it is the properties of signless integers that are being investigated, it is often convenient to work with positive and negative integers, and sometimes with a continuous variable, e.g. when using $\mathrm{li}\, x$. In more advanced developments complex numbers are used.

Factor Theorems. Two integers a and b are called co-prime if there is no integer that is a factor of both; or, we may say that *a is prime to b* or that *b is prime to a*. The fundamental theorem

if a and b are co-prime, then integers p, q exist such that $ap+bq=1$, and hence, if a and b are positive, positive integers P, Q exist such that $|\, aP-bQ\,|=1$,

may be proved by an argument similar to that on page 265. The H.C.F. process gives a set of equations

$$a=bq+r \quad b=rq_1+r_1 \quad r=r_1q_2+r_2 \ \ldots$$

from which it follows in succession that any factor of a, b is a factor of r, r_1, r_2, ... Also $r>r_1>r_2>\ldots$, so that a remainder r_n is eventually reached which is either 0 or 1. But if $r_n=0$, $r_{n-2}=r_{n-1}q_n$ and hence r_{n-1} is a factor of r_{n-2}; hence also of r_{n-3}, etc., and of a and b. Thus if a, b are co-prime, $r_n=1$. But each remainder is of the form $ap+bq$; hence $1=ap+bq$.

A similar argument may be used to show that

if a, b are co-prime and c is a factor of ad and b, then c is a factor of d.

For the equations that arise from the H.C.F. process give

$$da=dbq+dr \quad db=drq_1+dr_1 \quad dr=dr_1q_2+dr_2 \ \ldots$$

and it follows in succession that c is a factor of dr, dr_1, dr_2, ..., dr_n; but $dr_n=d$.

In particular, putting $c=b$, we have the result that

if b is a factor of da and is prime to a, then b is a factor of d.

Other properties of divisibility can be deduced from these theorems or can be proved by similar methods. It is suggested that the following should be discussed orally:

(i) If k is prime to a and to b, prove that it is prime to ab.
[If c is a factor of ab and k, and k is prime to a, then c is a factor of b.]

(ii) If k is a factor of a^n, prove that k is not prime to a.
[If k was prime to a, it would be prime to a^n by applications of (i) with $b = a, a^2, a^3, \ldots$.]

(iii) If p is a prime factor of a^n, prove that it is a factor of a.
[Since p is prime, if p is not a factor of a, p is prime to a, whereas by (ii) p is not prime to a.]

(iv) If a, b, c are each prime to all of x, y, z, w, prove that abc and $xyzw$ are co-prime.
[By repeated applications of (i).]

(v) If a is prime to b, prove that a^m is prime to b^n.
[By repeated applications of (i).]

(vi) If N is divisible by co-primes p, q, prove that it is divisible by pq.
[$N = pk$ and pk is divisible by q, but q is prime to p, therefore q is a factor of k, so $k = qr$ and $N = pqr$.]

Uniqueness of Factorisation. *Any positive integer N can be expressed in one and only one way in the form $2^{m_1}3^{m_2}5^{m_3}\ldots p_n^{m_n}$, where p_n is the n^{th} prime number and m_r is a positive integer or zero and $m_n \neq 0$.*

First, N is divided by 2 if possible, then the quotient is divided by 2 if possible, and so on, which gives $N = 2^{m_1}N_1$ where m_1 is a positive integer or zero and N_1 is not divisible by 2. Similarly $N_1 = 3^{m_2}N_2$ where N_2 is not divisible by 2 or 3, $N_2 = 5^{m_3}N_3$, and so on. Thus after a finite number of operations

$$N = 2^{m_1}3^{m_2}5^{m_3}\ldots p_n^{m_n} \equiv \prod_{r=1}^{n} p_r^{m_r}$$

where p_r denotes the r^{th} prime number.

To prove the uniqueness, let

$$2^{\alpha}3^{\beta}5^{\gamma}\ldots = N = 2^{\lambda}3^{\mu}5^{\nu}\ldots;$$

now if b is a factor of da and is prime to a, b must be a factor of d; but 2^{λ} is a factor of N and is prime to $3^{\beta}5^{\gamma}\ldots$; hence it is a factor of 2^{α}. Therefore $\lambda \leqslant \alpha$. Similarly $\alpha \leqslant \lambda$; hence $\alpha = \lambda$. Similarly $\beta = \mu$, $\gamma = \nu$, etc.

Divisors of N. The numbers by which N is exactly divisible are called the *divisors* of N. Unity is included as one of the divisors, and sometimes the number itself is included.

If $N = \prod_1^n p_r^{m_r}$, there are $\prod_1^n (1 + m_r)$ divisors of N including both 1 and N.

Each term of the expansion of

$$\prod_1^n (1 + p_r + p_r^2 + \ldots + p_r^{m_r})$$

is a divisor, every divisor is one term of the expansion, and the terms of the expansion are all different. Hence the number of divisors (including both 1 and N) is the number of terms, namely $\prod_1^n (1 + m_r)$.

For the *sum of the divisors*, see Exercise XIXa, No. 3.

EXERCISE XIXa

A

1. Find the number of divisors of 360 excluding 1 and 360.

2. If $N = \prod_{r=1}^n q_r^{m_r}$ where each q_r is prime, prove that N can be expressed as a product of two factors (counting 1, N as one pair) in $\frac{1}{2}\{1 + \prod_1^n (1 + m_r)\}$ ways or $\frac{1}{2}\prod_1^n (1 + m_r)$ ways according as N is or is not a perfect square. Apply the results to 360 and 4356.

3. With the notation of No. 2, prove that the sum of the divisors of N (including 1 and N) is $\prod\{(q_r^{m_r+1} - 1)/(q_r - 1)\}$ for $r = 1$ to n.

4. Use No. 3 to verify that 220 and 284 are *amicable* numbers, i.e. that each is the sum of the divisors of the other (including 1 but excluding the number itself).

5. Verify that 2, 4, 6, 12, 24 are the first five *highly composite* numbers, i.e. that each has more divisors than any number less than itself. Also find the sixth highly composite number.

6. Find the least number which has 28 divisors, excluding 1 and the number itself.

7. Prove that a polynomial in x with integral coefficients cannot be a prime number for all integral values of x. Extend the result to polynomials with fractional coefficients.

8. Verify that $n!+2$, $n!+3$, ..., $n!+n$ are $n-1$ consecutive composite numbers and if $n>2$ write down a set of n consecutive composite numbers smaller than those obtained by writing $n+1$ for n.

9. Evaluate $\dfrac{p_n}{n \log n}$ and $\dfrac{p_n}{n(\log n + \log\log n)}$ approximately for $n=10, 20$, given $p_{20}=71$. (It is interesting to note that $p_{100}=541$, and that the corresponding approximations are 1·17, ·88.)

10. Deduce from the prime number theorem that $\pi(2x)/\pi(x)$ tends to 2 when $x \to \infty$.

B

11. If $N=\prod_{r=1}^{n} q_r^{m_r}$ where each q_r is prime and no m_r is zero, prove that N can be expressed as the product of two co-prime factors in 2^{n-1} ways including 1, N as a co-prime pair. In how many ways can 360 be so expressed?

12. If a, b are co-prime, prove that $(a+b)^m$, $(a-b)^m$ are either co-prime or have 2^m as H.C.F.

13. If the smallest prime factor of n is greater than $\sqrt[3]{n}$, prove that n is the square of a prime or the product of two unequal primes.

14. Find the least positive integer n for which n^2+n+17 is composite.

15. Verify that 6, 28, 496 are perfect numbers. (A *perfect* number is one that is equal to the sum of its divisors, including 1 and excluding the number itself.)

16. Find approximate values of $\frac{\pi(x)}{x/\log x}$ and $\frac{\pi(x)}{\text{li}\, x}$ for $x = 10^7$ given $\pi(10^7) = 664579$ and $\text{li}\,(10^7) \doteq 664918$.

17. Excluding unity and the number itself, find the number of divisors of the highly composite number 6,746,328,388,800. [This number is $2^6.3^4.5^2.7^2.11.13.17.19.23$.]

18. If p and q are odd primes, find the sum of the divisors of $2^n p$ and of $2^n pq$, including 1 but excluding the number itself.

C

19. If $2^k - 1$ is prime, prove that $2^{k-1}(2^k - 1)$ is a perfect number. (See No. 15.)

20. If p_r is the r^{th} prime number, prove that $p_1 p_2 \ldots p_n - 1$ is either prime or divisible by a prime of the form $6m - 1$.

21. If N has n divisors including itself and 1, prove that their continued product is $\sqrt{N^n}$.

22. If $\prod_r q_r^{m_r}$ is highly composite where each q_r is prime, prove that the sequence (m_r) is monotone decreasing and that q_r is the r^{th} prime.

23. Prove that the r^{th} prime number is less than 2^n where $n = 2^r$.

24. Deduce from the prime number theorem

$$\text{(i)} \quad \lim_{x\to\infty} \frac{\pi(x + ax) - \pi(x)}{\pi(x)} = a$$

$$\text{(ii)} \quad \lim_{x\to\infty} \pi(x + ax) - \pi(x) = +\infty$$

25. If a, b, n are co-prime and $n < ab$, show how to express n/ab in the form $q/a + r/b$ where q, r are integers numerically less than a, b respectively.

26. Prove that the chance that two integers selected at random should be co-prime is $\prod_{r=1}^{\infty}\left(1 - \frac{1}{p_r^2}\right)$ where p_r is the r^{th} prime and evaluate this by means of $\sum_1^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

(Assume that if N is an integer chosen at random and p is prime, all remainders when N is divided by p are equally likely.)

The Integer Function. The greatest integer that is not greater than x is denoted by $[x]$.

For example $[5\frac{3}{4}]=5$, $[7]=7$, $[-\frac{3}{2}]=-2$, $[\frac{2}{3}]=0$.

It follows at once that $[x+y]$ is equal to $[x]+[y]$ or else to $[x]+[y]+1$. Hence $[x+y]\geqslant[x]+[y]$.

Also if f, n are positive integers, the number of multiples of f that are not greater than n is $\left[\frac{n}{f}\right]$; this includes f as one multiple.

If p is prime, the highest power of p which is a factor of $n!$ is p^x where

$$x=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$$

For $[n/p]$ of the integers $1, 2, 3, \ldots, n$ are divisible by p, $[n/p^2]$ of them are divisible by p^2, $[n/p^3]$ of them by p^3, and so on. Therefore the power to which p occurs in the product $1.2.3 \ldots n$ is the sum of $[n/p]$, $[n/p^2]$, $[n/p^3]$, ...

This series for x is terminated, because $[n/p^k]=0$ whenever $p^k>n$.

The product of r consecutive integers is divisible by $r!$

Denote the product by $(n+1)(n+2)\ldots(n+r)$. This is equal to $\frac{(n+r)!}{n!}$, and it is necessary to prove that $\frac{(n+r)!}{n!\,r!}$ is an integer. This follows from page 11 because $\frac{(n+r)!}{n!\,r!}$ is the number of ways in which n things can be selected from $n+r$ different things.

Alternatively it may be shown that any prime number p which occurs in $n!\,r!$ occurs to at least as high a power in $(n+r)!$ For $[x+y]\geqslant[x]+[y]$ shows that

$$\left[\frac{n+r}{p^k}\right]\geqslant\left[\frac{n}{p^k}\right]+\left[\frac{r}{p^k}\right]$$

and the result follows by putting $k=1, 2, 3, \ldots$, adding, and using the result of the previous paragraph.

There is much variety in the questions that can arise about numbers and their divisors, and also in the methods that can be applied.

To prove that N is a multiple of pq where p, q are co-prime, it is sufficient to show that N is a multiple of each separately. See (vi), p. 483.

In dealing with a divisor d, it is often convenient to use the fact that N can be expressed in the form $kd \pm r$, where k is integral and r is $0, 1, 2, \ldots, [\frac{1}{2}d]$.

Other methods are illustrated in Examples 1, 2, 3. The notation $M(k)$ or $N(k)$ is sometimes used for a multiple of k. It will be assumed that n is a positive integer, and the convention will be extended to other letters occasionally when the meaning is clear from the context.

Example 1. Prove that $3^{2n-1}+2^{n+1}$ is divisible by **7.**

First method. $3(3^{2n-1}+2^{n+1}) = 3^{2n}+6.2^n$

$$= 9^n - 2^n + 7.2^n.$$

But $9-2$ is a factor of $9^n - 2^n$ and hence 7 is a factor of

$$3(3^{2n-1}+2^{n+1})$$

and therefore of $3^{2n-1}+2^{n+1}$.

Second method. The remainders when $3^1, 3^2, 3^3, 3^7, \ldots$ are divided by 7 are 3, 6, 5, 3, 6, 5, ...; and the remainders for $2^2, 2^3, 2^4, 2^5, \ldots$ are 4, 1, 2, 4, 1, 2, ... These facts are easily discovered by trial. They may be proved by such arguments as these:

$$\text{if } 3^k = M(7)+3, \quad 3^{k+3} = 9M(7)+27 = N(7)+6$$

$$\text{if } 2^k = M(7)+4, \quad 2^{k+1} = 2M(7)+8 = N(7)+1.$$

Addition of the corresponding remainders 3, 4 and 6, 1 and 5, 2 shows that there is no remainder when $3^1+2^2, 3^3+2^3, 3^5+2^4, \ldots$ are divided by 7.

Example 2. Prove that $n(n+1)(2n+1)$ is divisible by 6.

First method. $n(n+1)(2n+1) = 2n(n+1)(n+2) - 3n(n+1)$.

Either n or $n+1$ is divisible by 2 and either n or $n+1$ or $n+2$ is divisible by 3. Hence the expression is divisible by 2×3.

Second method. $\frac{1}{6}n(n+1)(2n+1) = 1^2 + 2^2 + \ldots + n^2$, hence $n(n+1)(2n+1)$ is divisible by 6.

Example 3. Prove that $4^n - 18n^2 + 42n + 80$ is divisible by 108.

First method. If $f(n) = 4^n - 18n^2 + 42n + 80$,

$$f(n+1) - 4f(n) = 4^{n+1} - 18(n+1)^2 + 42(n+1) + 80 - 4^{n+1} + 72n^2 - 168n - 320$$
$$= 54n^2 - 162n - 216 = 54(n+1)(n-4).$$

But one of the numbers $n+1$, $n-4$ is even; hence

$$f(n+1) - 4f(n)$$

is divisible by 108. Therefore if $f(n)$ is divisible by 108, so also is $f(n+1)$.

But $f(1) = 108$, $\therefore f(2) = M(108)$, $\therefore f(3) = N(108)$, and so on.

Second method. $2.4^n = 2(1+3)^n = 2 + 6n + 9n(n-1) + M(27)$

$$\therefore 2f(n) = 9n^2 - 3n + 2 - 36n^2 + 84n + 160 + M(27)$$
$$= -27n^2 + 81n + 162 + M(27) = N(27).$$

Hence $2f(n)$, and so also $f(n)$, is divisible by 27.

Also $f(n) = 4^n - 60n^2 + 42n(n+1) + 80$ is divisible by 4 because $n(n+1)$ is even. Hence $f(n)$ is divisible by 108.

The Indicator. The number of positive integers including unity, which are less than n and prime to n, is called the *indicator* of n and is denoted by $\phi(n)$.

For example $\phi(2) = 1$, and $\phi(6) = 2$ since 1 and 5 are the only numbers less than 6 and prime to it.

A convention is made that $\phi(1) = 1$.

If $q_1, q_2, \ldots$ are the prime factors of N, so that $N = \prod_1^n q_r^{m_r}$ where $m_r \neq 0$, then

$$\phi(N) = N \prod_1^n \left(1 - \frac{1}{q_r}\right).$$

We start by finding the number of integers less than N and not prime to it. There are amongst the numbers not greater than N

(i) N/q_r multiples of q_r

(ii) $N/(q_r q_s)$ multiples of $q_r q_s$

(iii) $N/(q_r q_s q_t)$ multiples of $q_r q_s q_t$

and so on. It follows that the number of integers not greater than N and not prime to N (excluding unity) is

$$\Sigma N/q_r - \Sigma N/(q_r q_s) + \Sigma N/(q_r q_s q_t) - \ldots$$

To prove this, consider any integer not greater than N. Suppose that it is divisible by exactly k of the primes $q_1, q_2, \ldots, q_n$. This integer occurs k times in group (i), $\binom{k}{2}$ times in group (ii), $\binom{k}{3}$ times in group (iii), and so on. Therefore the number of times it is counted in the expression stated above is

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \ldots$$

which is equal to $1 - (1-1)^k$, i.e. 1. Therefore every integer (excluding unity) not greater than N and not prime to it is counted exactly once in the expression. Therefore since unity is counted in evaluating $\phi(N)$,

$$\begin{aligned}\phi(N) &= N - \{\Sigma N/q_r - \Sigma N/(q_r q_s) + \Sigma N/(q_r q_s q_t) - \ldots\} \\ &= N\{1 - \Sigma 1/q_r + \Sigma 1/(q_r q_s) - \Sigma 1/(q_r q_s q_t) + \ldots\} \\ &= N\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_n}\right).\end{aligned}$$

If $N = ab$ and a, b are co-prime, then $\varphi(N) = \varphi(a)\varphi(b)$

If the primes which are factors of a are $\alpha_1, \alpha_2, \ldots, \alpha_m$ and those which are factors of b are $\beta_1, \beta_2, \ldots, \beta_n$, then all the primes $\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n$ are unequal because a, b are co-prime.

But $$\phi(a)=a\prod_1^m\left(1-\frac{1}{\alpha_r}\right) \quad \phi(b)=b\prod_1^n\left(1-\frac{1}{\beta_r}\right)$$

and $$\phi(ab)=ab\prod_1^m\left(1-\frac{1}{\alpha_r}\right)\prod_1^n\left(1-\frac{1}{\beta_r}\right)$$

by the preceding result, and hence $\phi(ab)=\phi(a)\phi(b)$.

In the same way or by repeated application of this result it follows that

$$\varphi(a_1 a_2 \dots a_n)=\varphi(a_1)\varphi(a_2)\dots\varphi(a_n)$$

where $a_1, a_2, \dots, a_n$ are co-prime.

Example 4. Prove that the sum of the integers less than N and prime to it including unity is $\frac{1}{2}N\phi(N)$.

If x is an integer less than N and prime to it, so also is $N-x$. Hence such integers occur in pairs, whose sum is N and the number of pairs is $\frac{1}{2}\phi(N)$. Therefore the sum of the numbers is $\frac{1}{2}N\phi(N)$.

EXERCISE XIXb

A

1. Sketch the graphs of $[x]$ and $x-[x]$.

2. If n is an integer, find the values of x for which

$$[x]+[n-x]=n-1.$$

3. Find the greatest power of 7 which is a factor of 1000!

4. Find the number of positive integers including unity which are less than 9000 and prime to it.

Prove the statements in Nos. 5-12.

5. $n^3+5n=M(6)$.

6. $17^{2n}-1=M(288)$.

7. $3^{2n+4}-2^{2n}=M(5)$.

8. $2^{n+2}+3^{2n+1}=M(7)$.

9. $4^n+6n-1=M(9)$.

10. $n(n+1)(2n+1)(3n^2+3n-1)=M(30)$.

11. $(2m)!(2n)!$ is divisible by $m!\,n!(m+n)!$

12. $(2n)!$ is divisible by $n!(n+1)!$

B

13. Find the number of zeros at the end of the number which equals 1000!

Prove the statements in Nos. 14-19

14. $n^3 + 3n = M(2)$.

15. $n^4 + 2n^3 - 3 = M(32)$ if n is odd.

16. $23^{2n} - 1 = M(528)$.

17. $13^{2n+1} + 9^{n+1} = M(22)$.

18. $7^{4n} - 48n - 1 = M(2304)$.

19. $3^{2n+2} - 8n - 9 = M(64)$.

20. Explain why the numbers less than 30 and prime to it must all be prime.

21. Find the sum of the positive integers including unity which are less than 600 and prime to it.

22. If n is a positive integer, prove that $[[x]/n] = [x/n]$.

C

23. Prove that the number of positive integers less than 65^m which are divisible by 8 and not by 64 is $\frac{7}{64}(65^m - 1)$.

24. How many numbers including unity are less than 210 and prime to it but are not themselves prime?

25. If $S(x)$ denotes the sum of the divisors of x including 1 and x, and if m, n are co-prime, prove that $S(m)S(n) = S(mn)$.

26. If $a, b, c, \ldots$ are the integers less than n and prime to it, prove that Σa, Σabc, $\Sigma abcde$, ... are multiples of n.

27. If $N = \prod_1^\sigma q_r^{m_r}$, prove that the sum of the squares of the numbers less than N and prime to it is

$$\tfrac{1}{3}N^3\Pi(1 - q_r^{-1}) + \tfrac{1}{6}N\Pi(1 - q_r).$$

28. Prove that the sum of the cubes of the numbers less than N and prime to it is, with the notation of No. 27,

$$\tfrac{1}{4}N^4\Pi(1 - q_r^{-1}) + \tfrac{1}{4}N^2\Pi(1 - q_r).$$

29. If n is the product of positive integers p and q, prove that there are $\phi(q)$ integers less than n which have with n the H.C.F. p.

30. Use No. 29 to prove Gauss' Theorem that $\Sigma\phi(d) = n$, where the summation extends to all the divisors d of n, including 1 and n.

31. If d is a divisor of $\Pi q_r^{m_r}$, prove that

$$\Sigma\phi(d) = \Pi\{1 + \phi(q_r) + \phi(q_r^2) + \ldots + \phi(q_r^{m_r})\}$$

and deduce the result of No. 30.

32. If $s(n)$ is the sum of the digits of the number n when expressed in the scale of k, and $Q(n)$ is the highest power of k which is a factor of $n!$, show that $(k-1)Q(n) = n - s(n)$.

Also prove (i) $s(n+m) \leqslant s(n) + s(m)$

(ii) $s(rn) \leqslant rs(n)$

(iii) $s(k^r n) = s(n)$

and deduce that $s(nm) \leqslant s(n)s(m)$.

Congruences. Two integers a and b are called *congruent* with respect to the modulus m if an integer k exists such that

$$a - b = km.$$

k may be positive, zero, or negative. The congruence is denoted by $a \equiv b \pmod{m}$ or by $a - b \equiv 0 \pmod{m}$. a and b are also called *equal (mod m)*.

For example $10 \equiv 3 \pmod{7}$, and $13 \equiv 28 \pmod{5}$. Also $a \equiv b \pmod{p}$ if $a = b + kp$.

Sometimes the notation is used in a wider sense: the general solution of $\tan\theta = \tan\alpha$ may be written $\theta = \alpha \pmod{\pi}$.

It will be shown that the calculus of congruences is so like that of equations that no inconvenience arises from using the same notation for both. The explicit statement of the modulus at each stage of the work is not necessary when the same modulus is used throughout. See Examples 6, 7, 8.

If $a \equiv b \pmod{m}$ and $a' \equiv b' \pmod{m}$ and if q, r are integers, then

$$\text{(i) } qa + ra' \equiv qb + rb' \pmod{m} \qquad \text{(ii) } aa' \equiv bb' \pmod{m}.$$

(i) $a - b = km$, $a' - b' = k'm$ where k, k' are integers.

$$\therefore\ q(a-b) + r(a'-b') = (qk + rk')m$$

$$\therefore\ qa + ra' = qb + rb' + M(m)$$

$$\therefore\ qa + ra' \equiv qb + rb' \pmod{m}.$$

(ii) $a = b + km$, $a' = b' + k'm$.

$$\therefore\ aa' = bb' + m(kb' + k'b + mkk')$$

$$\therefore\ aa' \equiv bb' \pmod{m}.$$

These results show that congruences may be manipulated as regards addition, subtraction, and multiplication, with integral numbers, just like equations.

As regards division a modification is necessary.

From $26 = 12 \pmod 7$, it follows that $13 = 6 \pmod 7$, but $91 = 35 \pmod{14}$ only implies that $13 = 5 \pmod 2$ and not that $13 = 5 \pmod{14}$.

In general if $ax = bx \pmod m$ and if h is the H.C.F. of x, m, then $a = b \pmod{m/h}$.

$$x = ph, \ m = qh, \text{ where } p, q \text{ are co-prime.}$$

Since $ax - bx = km$, $aph - bph = kqh$,

$$\therefore \ p(a-b) = kq.$$

But q is prime to p and is therefore a factor of $a - b$. Thus $a = b \pmod q$, i.e. $a = b \pmod{m/h}$.

In particular, if x, m are co-prime, $a = b \pmod m$.

Example 5. Prove that $3^{4n+2} + 5^{2n+1}$ is divisible by 14.

$$3^{4n+2} = 9.81^n = 9.11^n \pmod{14}$$

and $$5^{2n+1} = 5.25^n = 5.11^n \pmod{14}$$

thus $$3^{4n+2} + 5^{2n+1} = 14.11^n = 0 \pmod{14}.$$

Comparison of this example with Example 1, p. 488, shows that the congruence notation often shortens the work. It also helps by suggesting the procedure to be adopted.

Example 6. Find the remainder when 2^{1000} is divided by 13.

Since $2^3 = 8$, $2^4 = 64 = -1 \pmod{13}$,

thus $2^{996} = (-1)^{166} = +1$, $\therefore \ 2^{1000} = 2^4 = 16 = 3 \pmod{13}$,

thus the remainder is 3.

Congruences are often used as in Example 6 for calculating the remainder in a given division.

Amongst the numbers which are congruent to $a \pmod m$, there is one, x, which satisfies $0 < x < m$, assuming $a \neq 0 \pmod m$. This is called the **least positive residue of** $a \pmod m$.

If a and m are co-prime, and the m positive integers

$$k,\ k+a,\ k+2a,\ \dots,\ k+(m-1)a$$

are divided by m, the remainders are a permutation of $0, 1, 2, \dots, m-1$.

In a division by m, these are the only possible remainders. Hence it is sufficient to show that no two of the m numbers can leave the same remainder.

If $k+ra$, $k+sa$ leave the same remainder when r, s each have one of the values $0, 1, 2, \dots, m-1$,

$$k+ra \equiv k+sa \pmod{m}$$
$$\therefore\ ra \equiv sa \pmod{m}.$$

But a and m are co-prime; hence $r \equiv s \pmod{m}$ from which it follows that $r=s$ because $|r-s| \leqslant m-1$.

The result may be stated in the form:

one of the numbers $k,\ k+a,\ \dots,\ k+(m-1)a$ is divisible by m and the least positive residues of the others are all different.

For the corresponding theorem when a, m are not co-prime see Exercise XIXc, No. 45.

The reader should now work Exercise XIXc, Nos. 1-6.

Degree of a Congruence. The congruence

$$A_0x^n + A_1x^{n-1} + \dots + A_n \equiv 0 \pmod{m}$$

where $A_0, A_1, \dots, A_n$ are integers is said to be of *degree* n provided that $A_0 \not\equiv 0 \pmod{m}$.

A value of x which satisfies the congruence is called a *root* of the congruence. If x is a root and $x' \equiv x \pmod{m}$, then x' is also a root. The solution of a congruence consists in finding as many values of x as possible, which satisfy the congruence and are incongruent to one another (mod m).

If $A_0 \equiv A_1 \equiv \dots \equiv A_n \equiv 0 \pmod{m}$ the congruence is satisfied by all values of x and is called an *identical congruence*.

The coefficients $A_0, A_1, \dots, A_n$ of any congruence may always be replaced by coefficients $a_0, a_1, \dots, a_n$ which are positive integers less than m, or zero. For A_k may be replaced by its least positive residue (mod m) or else by zero. Also if the congruence is of degree n, $a_0 \not\equiv 0$, because $A_0 \not\equiv 0 \pmod{m}$.

In the following discussion we consider only congruences for which the modulus is a *prime* number p, though a few examples of a composite modulus are given in Exercise XIXc.

Congruences of the First Degree. *Every congruence of the first degree with a prime modulus has one root and cannot have two incongruent roots.*

The congruence may be written $ax \equiv b \pmod{p}$, where a, b are positive integers less than p or zero. Also $a \not\equiv 0$ by the definition of degree.

By the theorem on page 495, $0, a, 2a, \ldots, (p-1)a$ are congruent (mod p) to some permutation of $0, 1, 2, \ldots, p-1$. Hence one and only one of them is b, i.e. one and only one of the values $0, 1, 2, \ldots, p-1$ of x makes $ax \equiv b \pmod{p}$ and is a root of the congruence.

A congruence of degree n with a prime modulus p cannot have more than n incongruent roots.

The congruence may be written

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$$

where $0 < a_0 < p$, $0 \leqslant a_r < p$ for $r = 1$ to n.

Let x_1 be a root. Then

$$a_0x_1^n + a_1x_1^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$$

and any root satisfies also

$$a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + \ldots + a_{n-1}(x - x_1) \equiv 0 \pmod{p};$$

i.e. $$(x - x_1)(a_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) \equiv 0 \pmod{p}.$$

As p is prime this can only be true if p is a factor of $x - x_1$ or of $a_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}$. Hence if $x \not\equiv x_1 \pmod{p}$, x can only satisfy the given congruence if it satisfies

$$a_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1} \equiv 0 \pmod{p}.$$

If therefore we assume that a congruence of degree $n-1$ cannot have more than $n-1$ incongruent roots, it follows that a congruence of degree n cannot have more than n incongruent roots. But a congruence of degree 1 cannot have 2 incongruent roots; hence it follows by induction that a congruence of degree n cannot have more than n incongruent roots.

Methods of solving congruences of degrees 1 and 2 are illustrated in Examples 7-10. These congruences are called simple (or linear) and quadratic respectively.

Example 7. Solve $106x \equiv 5 \pmod{137}$.

In the process for finding the H.C.F. of 106, 137, the successive remainders are 31, 13, 5, 3, 2, 1, and therefore the coefficient of x in the given congruence can be reduced successively to these values.

3	106	137	1
	93	106	
2	13	31	2
	10	26	
1	3	5	1
	2	3	
	1	2	

$-31x \equiv 5$, $\therefore$ $-93x \equiv 15$;

but $106x \equiv 5$, $\therefore$ $13x \equiv 20$; $\therefore$ $26x \equiv 40$;

but $-31x \equiv 5$, $\therefore$ $-5x \equiv 45$, $\therefore$ $-10x \equiv 90$;

but $13x \equiv 20$, $\therefore$ $3x \equiv 110$;

but $-5x \equiv 45$, $\therefore$ $-2x \equiv 155 \equiv 18$;

but $3x \equiv 110$, $\therefore$ $x \equiv 128 \pmod{137}$.

The work can however often be shortened. In this example, since $-5x \equiv 45$, and since 137 and 5 are co-prime,

$$x \equiv -9 \equiv 128 \pmod{137}$$

Alternatively, express $\frac{137}{106}$ as a continued fraction and calculate the last convergent but one. It is shown on p. 244 that this is $\frac{53}{41}$. Therefore from p. 245, $53.106 - 41.137 = 1$,

$\therefore$ $53.106 \equiv 1 \pmod{137}$, $\therefore$ $265.106 \equiv 5 \pmod{137}$;

$\therefore$ $106x \equiv 5 \pmod{137}$ is satisfied by $x \equiv 265 \equiv 128 \pmod{137}$.

Note. The method of Example 7 can be applied to Example 17, p. 246, because y is given by the congruence $106y \equiv -4 \pmod{137}$.

Example 8. Solve $98x \equiv 1 \pmod{139}$.

$$98x \equiv 1 \equiv 140,$$

but 14 and 139 are co-prime,

$$\therefore 7x \equiv 10 \equiv 10 + 3.139 \equiv 427,$$

$$\therefore x \equiv 61 \pmod{139}.$$

Example 9. Prove that $13x^2 = a \pmod 5$ has no solution if $a = 1$ or $4 \pmod 5$, and solve it for $a = 2$ or $3 \pmod 5$.

$13x^2 = 3x^2 \pmod 5$, and its values for $x = 0, 1, 2, 3, 4 \pmod 5$ are respectively 0, 3, 12, 27, 48, i.e. 0, 3, 2, 2, 3, $\pmod 5$.

This shows that $13x^2 = a \pmod 5$ is never true if $a = 1$ or $4 \pmod 5$, and that the solutions for $a = 2, 3 \pmod 5$ are respectively $x = 2$ or $3 \pmod 5$ and $x = 1$ or $4 \pmod 5$.

In Example 9, the solutions of $13x^2 = 2$ or $3 \pmod 5$ may also be found as follows:

$3x^2 = 2 = 12$; but 3, 5 are co-prime, $\therefore x^2 = 4$,

$\therefore x = \pm 2 = 2$ or $3 \pmod 5$.

$3x^2 = 3$; but 3, 5 are co-prime, $\therefore x^2 = 1$,

$\therefore x = \pm 1 = 1$ or $4 \pmod 5$.

The positive values of a less than p for which $x^2 = a \pmod p$ has solutions are called *quadratic residues* $\pmod p$; the values of a for which it has no solutions are called *non-residues* $\pmod p$. Thus 1, 4 are quadratic residues $\pmod 5$ and 2, 3 are non-residues. It will be proved later (p. 504) that if p is an odd prime there are $\frac{1}{2}(p-1)$ residues and $\frac{1}{2}(p-1)$ non-residues $\pmod p$.

The process of reducing any quadratic congruence to the form $x^2 = a \pmod p$ is illustrated by Example 10, and if a is a quadratic residue $\pmod p$, this may be written in the form $x^2 = b^2 \pmod p$. It is then legitimate to say that the *general solution* is $x = \pm b \pmod p$, because there cannot be more than two incongruent roots, and these two values of x are incongruent and satisfy the congruence.

Example 10. Solve $3x^2 + 4x = 10 \pmod{17}$.

The process consists in reducing the coefficient of x^2 to unity and that of x to an even number:

$$3x^2 + 4x - 10 = 3x^2 + 72x + 24 = 3(x^2 + 24x + 8).$$

But 17 and 3 are co-prime, $\therefore x^2 + 24x + 8 = 0$,

$\therefore (x+12)^2 = 144 - 8 = 136 = 0$, $\therefore x = -12 = 5 \pmod{17}$.

The congruence in Example 10 is said to have *equal roots*.

EXERCISE XIXc

A

Prove the congruences in Nos. 1-4.

1. $n^5 - n = 0 \pmod{30}$
2. $3.5^{2n+1} + 2^{3n+1} = 0 \pmod{17}$
3. $n(n-1)(n+25)(n+50) = 0 \pmod{24}$
4. $n(n^2-1)(29n^2+4) = 0 \pmod{120}$

Find the least positive residues in Nos. 5, 6.

5. $2^{41} \pmod{23}$
6. $18^{96} \pmod{11}$

Solve the congruences in Nos. 7-18.

7. $2x = 1 \pmod{5}$
8. $31x = 1 \pmod{71}$
9. $12x = 6 \pmod{5}$
10. $12x = 6 \pmod{30}$
11. $x = 3 \pmod{7} = 5 \pmod{11}$
12. $x^2 = 15 \pmod{17}$
13. $2x^2 = 3 \pmod{19}$
14. $x^2 + 2 = 0 \pmod{7}$
15. $x^2 + 4x = 22 \pmod{23}$
16. $5x^2 + 7x = 24 \pmod{47}$.
17. $2x^2 + x = 2 \pmod{19}$
18. $7x^2 = 3x + 2 \pmod{29}$

19. Give the non-residues (mod 11). Prove that $m^2 + n^2$ is only divisible by 11 if m and n are both divisible by 11.

20. Solve $5x^2 = a \pmod{7}$ for the values of a other than zero for which it is possible.

21. If $x_1, x_2, \ldots, x_n$ are incongruent roots of

$$f(x) \equiv a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0 \pmod{p}$$

where p is prime, prove that

$$a_0(x - x_1)(x - x_2) \ldots (x - x_n) = f(x) \pmod{p}$$

is an identical congruence, and deduce that

$$a_0 x_1 x_2 \ldots x_n = (-1)^n a_n \pmod{p}.$$

B

Prove the congruences in Nos. 22-26.

22. $3^{4n} = 1 \pmod{80}$
23. $37^{2n} = 1 \pmod{1368}$
24. $3^{44} = -40 \pmod{121}$
25. $3.4^{n+1} + 10^{n-1} = 4 \pmod{9}$
26. $3^{90} = 1 \pmod{91}$

27. Find the remainders when a, $2a$, $3a$, ... , pa are divided by m if the values of m, p, a are

(i) 7, 6, 5 (ii) 9, 3, 6 (iii) 12, 6, 10

Solve the congruences in Nos. 28-39.

28. $2x \equiv 3 \pmod 5$ 29. $5x \equiv 1 \pmod 7$

30. $2x \equiv 1 \pmod 3$ 31. $10x \equiv 5 \pmod 3$

32. $10x \equiv 5 \pmod{15}$ 33. $235x \equiv 46 \pmod{541}$

34. $31x \equiv 13 \pmod{71}$ 35. $51x \equiv 6 \pmod{39}$

36. $95x \equiv 57 \pmod{323}$ 37. $x^2 + x \equiv 43 \pmod{73}$

38. $x^3 + x \equiv 16 \pmod{101}$ 39. $2x^3 + 3x + 2 \equiv 0 \pmod{11}$

40. Give the quadratic residues (mod 13).

41. Prove the rule for testing divisibility by 11 in the scale of 10.

Find the least positive residues in Nos. 42-44.

42. $2^{37} \pmod{223}$ 43. $3^{16} \pmod{77}$

44. $19^{4n+3} \pmod{181}$

C

45. If the H.C.F. of a and m is h, and h is a factor of k, prove that the least positive residues (mod m) of the integers k, $k+a$, $k+2a$, ... , $k+a(m-h)/h$ are a permutation of 0, h, $2h$, ... , $m-h$. Also prove that the residues for further sets of m/h terms of the same A.P. are the same permutation.

46. If $(\ldots zyx)$ denotes the number $x + 10y + 10^2z + \ldots$ in the scale of ten, prove that $(\ldots cba)$ is divisible by 7 if

$$(cba) - (fed) + (ihg) - \ldots$$

is so divisible.

Show that the same test applies to 11 and 13.

47. For a number expressed in the scale of twelve, show that the same test for divisibility by 7 holds as in No. 46.

Find tests for divisibility by 5 in the scale of twelve and for divisibility by $k-1$ and $k+1$ in the scale of k.

48. Write down the general solutions of $x^2 \equiv 4 \pmod 5$ and $x^2 \equiv 4 \pmod 7$ and find their common roots. What congruence has these common roots as its complete solution?

49. Show that $x^2 = a \pmod{pq}$ where p, q are co-prime is possible if and only if $x^2 = a \pmod{p}$ and $x^2 = a \pmod{q}$ are both possible.

50. If x_1 is a root of $x^2 = a \pmod{p}$ where p is an odd prime and a is prime to p, prove that an integer k exists such that $x_1 + kp$ is a root of $x^2 = a \pmod{p^2}$. Hence solve $x^2 = 2 \pmod{49}$.

51. Show how to deduce solutions of $x^2 = a \pmod{p^{n+1}}$ from those of $x^2 = a \pmod{p^n}$, where p is an odd prime and a is prime to p.

52. Solve $x^2 = 1 \pmod{2^k}$ for $k = 2$, $k = 3$, $k > 3$.

Fermat's Theorem. If p is prime and a is prime to p, then

$$a^{p-1} = 1 \pmod{p}$$

By the theorem proved on page 495, a, $2a$, $3a$, ..., $(p-1)a$ are congruent (mod p) to 1, 2, 3, ..., $p-1$, in some order. Hence by the theorem (ii) on page 493,

$$a.2a.3a. \ldots (p-1)a = 1.2.3 \ldots p-1 \pmod{p}$$

$\therefore$ as p is prime to $1.2.3 \ldots p-1$,

$$a^{p-1} = 1 \pmod{p}.$$

An alternative proof is suggested in Exercise XIXd, No. 25.

The result may also be stated in the form

$$a^p = a \pmod{p}$$

which holds even when a is not prime to p.

A generalisation of Fermat's theorem, known as *Euler's extension*, applies to the case when p is not prime. This is proved by the same method as follows.

Let $q_1, q_2, \ldots, q_n$ be the $\phi(m)$ integers less than m and prime to it; $q_1 = 1$ and $n = \phi(m)$. Then if a is prime to m, $q_1 a, q_2 a, \ldots, q_n a$ are incongruent (mod m); for if $q_r a = q_s a \pmod{m}$, $q_r = q_s \pmod{m}$ and since $0 < |q_r - q_s| < m$, $q_r = q_s$. Also $q_k a$ is prime to m, and hence its least positive residue is prime to m. Hence these residues are $q_1, q_2, \ldots, q_n$ in some order. It follows as in Fermat's theorem that

$$q_1 a . q_2 a . \ldots q_n a = q_1 q_2 \ldots q_n \pmod{m}$$

and that $a^{\phi(m)} = 1 \pmod{m}$ **if a is prime to m.**

Wilson's Theorem. $(p-1)! \equiv -1 \pmod{p}$, **if and only if** p **is prime.**

By Fermat's theorem, if p is prime, the congruence

$$x^{p-1} - 1 = 0 \pmod{p}$$

is satisfied by $x = 1, 2, 3, \ldots, (p-1) \pmod{p}$. Therefore the congruence

$$(x-1)(x-2)(x-3)\ldots(x-p+1) - (x^{p-1}-1) = 0 \pmod{p}$$

is satisfied by the same $p-1$ incongruent values of x. But its degree does not exceed $p-2$. It must therefore be an identical congruence. Putting $x = 0$,

$$(-1)^{p-1}(p-1)! + 1 = 0 \pmod{p}$$

$\therefore$ if p is an odd prime, $(p-1)! \equiv -1 \pmod{p}$. This result holds also for $p = 2$.

If p is not prime, p and $(p-1)!$ are not co-prime; therefore $(p-1)!+1$ is not divisible by p.

Wilson's Theorem provides a necessary and sufficient test for a number to be prime, but this is of no practical value on account of the labour of calculating $(p-1)!$

In the identical congruence used in the proof, the coefficient of each power of x up to and including x^{p-2} must be zero $\pmod{p}$. This proves Lagrange's Theorem:

The sum of the products taken r at a time of the numbers $1, 2, 3, \ldots, p-1$ *is divisible by* p, *where* p *is prime and* $r \leqslant p-2$.

The following alternative proof of Wilson's Theorem was given by Cayley. See also Exercise XIXd, Nos. 33, 34.

Consider the $(p-1)!/2$ polygons of p sides which have their p vertices at the vertices of a regular polygon. Of these, $(p-1)/2$ are regular. But the irregular polygons can be grouped in sets of p obtained by rotating any such polygon about its centre through angles $2\pi/p$. Hence the number of irregular polygons is a multiple of p. Therefore

$$\tfrac{1}{2}\{(p-1)! - (p-1)\} = 0 \pmod{p}$$

$$\therefore (p-1)! = p - 1 = -1 \pmod{p}.$$

Fermat's Last Theorem. The theorem on p. 501 although stated by Fermat about 1670 was first proved by Euler in 1761 by a method substantially equivalent to that given in the text. Most of Fermat's discoveries were published without proofs. One of them, known as his 'last theorem' is of special interest. In the margin of a copy of Diophantus' Algebra which was edited by Fermat, he stated that he had found a general proof that the equation $x^n + y^n = z^n$ has no solution in integers if $n = 3, 4, 5, \ldots$

No complete proof of this has been discovered, although the impossibility has been proved for an unlimited number of values of n. This has been done by methods which were unknown to Fermat.

The equation $x^2 + y^2 = z^2$ is satisfied by $x = 2kab$, $y = k(a^2 - b^2)$, $z = k(a^2 + b^2)$, and it can be shown as follows that every integral solution can be expressed in this form where a, b, k are integers.

If k is a common factor of any two of x, y, z, it must also be a factor of the third, and x, y, z may be replaced by kX, kY, kZ where X, Y, Z are all co-prime and $X^2 + Y^2 = Z^2$.

Also X, Y cannot both be odd, for then $X^2 + Y^2 \equiv 2 \pmod 4$, and so $X^2 + Y^2 \neq Z^2$. Thus one of X, Y is odd and the other is even. Suppose X is even and Y odd; then Z is odd and $Z \pm Y$ are even.

Let $Z + Y = 2m$, $Z - Y = 2n$; then $(\frac{1}{2}X)^2 = mn$.

But Z, Y are co-prime, therefore m, n are co-prime. But mn is a square, therefore m, n are both squares. Thus $m = a^2$, $n = b^2$, and $X = 2ab$, $Y = a^2 - b^2$, $Z = a^2 + b^2$.

Therefore the general solution is

$$x = 2kab, \quad y = k(a^2 - b^2), \quad z = k(a^2 + b^2)$$

where a, b, k are integers.

Example 11. If x, y, z are integers such that $x^2 + y^2 = z^2$, prove that $xyz = 0 \pmod{60}$.

By the result just obtained,

$$xyz = 2k^3ab(a^2 - b^2)(a^2 + b^2) = 2k^3ab(a^4 - b^4)$$

where k, a, b are integers.

Either a, b, or $a^2 - b^2$ is even, $\therefore xyz = 0 \pmod 4$.

Either a or b is a multiple of 3, or by Fermat's theorem

$$a^2 - b^2 = 1 - 1 \pmod 3 = 0 \pmod 3; \quad \therefore xyz = 0 \pmod 3.$$

Similarly a or b is a multiple of 5, or $a^4 - b^4 = 0 \pmod 5$;

$$\therefore xyz = 0 \pmod 5. \quad \text{Thus } xyz = 0 \pmod{60}.$$

Quadratic Residues. *If p is an odd prime, there are $\frac{1}{2}(p-1)$ quadratic residues (mod p) and $\frac{1}{2}(p-1)$ non-residues.*

The residues are the positive values of $a (< p)$ for which $x^2 = a \pmod p$ is possible.

The values $1, 2, 3, \ldots, \frac{1}{2}(p-1)$ of x give $\frac{1}{2}(p-1)$ incongruent values of a. For if $r^2 = s^2 \pmod p$ where $0 < r \leqslant s \leqslant \frac{1}{2}(p-1)$,

$$(r+s)(r-s) = 0 \pmod p,$$

and since p is prime, p is a factor of $r+s$ or $r-s$. But

$$r - s < r + s < p;$$

thus $r = s$. Hence there are $\frac{1}{2}(p-1)$ quadratic residues. There cannot be more than $\frac{1}{2}(p-1)$ because $x_1^2 = (p - x_1)^2 \pmod p$, so that the values $\frac{1}{2}(p+1), \frac{1}{2}(p+3), \ldots, p-1$ of x lead to the same values of a as before.

If a is a residue, $a^{\frac{1}{2}(p-1)} = (x^2)^{\frac{1}{2}(p-1)} = 1 \pmod p$ by Fermat's theorem. The residues are the roots of this congruence of degree $\frac{1}{2}(p-1)$.

The non-residues must be the roots of the congruence

$$a^{\frac{1}{2}(p-1)} = -1 \pmod p,$$

because residues and non-residues satisfy

$$a^{p-1} - 1 \equiv \{a^{\frac{1}{2}(p-1)} - 1\}\{a^{\frac{1}{2}(p-1)} + 1\} = 0 \pmod p$$

by Fermat's theorem.

Example 12. If p is prime and x is prime to p, prove that

$$x^{p(p-1)/2} \equiv \pm 1 \pmod{p^2}.$$

If $p=2$, $x \equiv \pm 1 \pmod 4$ because x is prime to 2.

If p is an odd prime, let $y = x^{p-1}$. Then by Fermat's theorem $y \equiv 1 \pmod p$, $\therefore y^r \equiv 1 \pmod p$.

Hence

$$x^{p(p-1)} - 1 = y^p - 1 = (y-1)(y^{p-1} + y^{p-2} + \ldots + y + 1) \equiv 0 \pmod{p^2},$$

because $y - 1 \equiv 0 \pmod p$ and

$$y^{p-1} + y^{p-2} + \ldots + y + 1 = p \equiv 0 \pmod p.$$

Hence $(x^{p(p-1)/2} + 1)(x^{p(p-1)/2} - 1)$ is divisible by p^2. But since the two factors differ by 2, and $p \neq 2$, they cannot both be divisible by p. One of them must therefore be divisible by p^2. This shows that $x^{p(p-1)/2} \equiv \pm 1 \pmod{p^2}$.

Example 13. If a and b are co-prime, prove that $a^2 + b^2$ cannot have a factor of the form $4m+3$.

Let $2n+1$ be an odd prime factor of $a^2 + b^2$. Since a, b are co-prime, they are also prime to $a^2 + b^2$ and to $2n+1$.

Hence by Fermat's theorem

$$a^{2n} - b^{2n} \equiv 1 - 1 \equiv 0 \pmod{2n+1}.$$

Thus $a^2(a^{2n-2} + b^{2n-2}) \equiv a^{2n} - b^{2n} + b^{2n-2}(a^2 + b^2) \equiv 0$

and therefore $a^{2n-2} + b^{2n-2} \equiv 0 \pmod{2n+1}$.

Similarly $a^{2n-4} - b^{2n-4} \equiv 0 \pmod{2n+1}$,

and by repeating the process

$$a^2 + (-1)^n b^2 \equiv 0 \pmod{2n+1}.$$

But $2n+1$ is a factor of $a^2 + b^2$, and cannot also be a factor of $a^2 - b^2$ since a^2, b^2 are co-prime. Hence n is even, and every odd prime factor of $a^2 + b^2$ is of the form $4m+1$.

Since the product $(4k_1+1)(4k_2+1)\ldots(4k_r+1)$ is of the form $4k+1$, it follows that every odd factor of $a^2 + b^2$ is of the form $4k+1$.

When a, b are not co-prime, $a^2 + b^2$ may contain a factor $(4m+3)^r$ where r is even.

Example 14. If $2n+1$ is prime, prove that

$$(n!)^2 = (-1)^{n+1} \pmod{2n+1}.$$

By Wilson's theorem, $1.2.3 \ldots 2n = -1 \pmod{2n+1}$.

But

$2n = -1$, $2n-1 = -2$, $2n-2 = -3$, $\ldots$, $n+1 = -n$, (mod $2n+1$),

hence

$$1.2.3 \ldots n(-n)(-n+1) \ldots (-3)(-2)(-1) = -1 \pmod{2n+1}$$

i.e. $$(-1)^n (n!)^2 = -1 \pmod{2n+1}.$$

Alternatively, the congruence

$$x^{2n} - 1 - (x^2 - 1^2)(x^2 - 2^2) \ldots (x^2 - n^2) = 0 \pmod{2n+1}$$

is satisfied by the $2n$ incongruent values ± 1, ± 2, $\ldots$, $\pm n$, and is not of degree as great as $2n$. Therefore it is an identical congruence. Putting $x = 0$,

$$-1 = (-1)^n 1^2 . 2^2 \ldots n^2 = (-1)^n (n!)^2 \pmod{2n+1}.$$

Mersenne's Numbers. The only known perfect numbers are of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime. See Exercise XIXa, No. 19. In 1644, Mersenne asserted that the only prime values of n up to 257 for which $2^n - 1$ is prime are 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.

It has since been proved that $2^{67} - 1$ and $2^{257} - 1$ are composite and that $2^{61} - 1$, $2^{89} - 1$ and $2^{107} - 1$ are prime. Mersenne's statement has not been checked for 157, 167, 193, 199, 227, 229.

It is possible that Fermat and Mersenne used some method that has not been rediscovered.

EXERCISE XIXd

A

Prove the congruences in Nos. 1-9.

1. $n^4 = 1 \pmod{240}$ if n is prime to 30.

2. $n^{13} = n \pmod{78}$.

3. $m^{13} = n^{13} \pmod{91}$ if m, n are prime to 91.

4. $(qr)^{p-1} + (rp)^{q-1} + (pq)^{r-1} = 1 \pmod{pqr}$ if p, q, r are unequal primes.

5. $28! = 666 \pmod{899}$.

6. $2.(p-3)! \equiv -1 \pmod{p}$ if p is prime and >3.

7. $(p-r)!\,(r-1)! = (-1)^r \pmod{p}$ if p is prime and $>r$.

8. $16^{59} \equiv 1 \pmod{437}$. (Use Euler's theorem.)

9. $x^{pq-q} \equiv 1 \pmod{pq}$, if x is prime to p, p is prime, and $q = p^n$.

10. If x, y, z are integers such that $x^2 + y^2 = z^2$, prove that $xy(x^2 - y^2) \equiv 0 \pmod{84}$

11. If p is an odd prime, prove that

$$x^{p-1} - 1 = \{x^2 + 1(p-1)\}\{x^2 + 2(p-2)\} \ldots \{x^2 + \tfrac{1}{2}(p-1)\tfrac{1}{2}(p+1)\} \pmod{p}$$

is an identical congruence.

12. By verifying that $x^2 + y^2 + z^2 \not\equiv 7 \pmod{8}$, prove that no term of the A.P. 7, 15, 23, 31, ... is the sum of three squares.

B

Prove the congruences in Nos. 13-21.

13. $n^7 \equiv n \pmod{42}$

14. $(2n+1)^5 \equiv (2n+1) \pmod{240}$

15. $n^8 \equiv 1 \pmod{480}$ if n is prime to 30

16. $n^3 \equiv n \pmod{30}$ if $n > 3$ and $2n-1$, $2n+1$ are prime

17. $n^6 \equiv 1 \pmod{504}$ if n is prime to 42

18. $(p-2)! \equiv 1 \pmod{p}$ if p is an odd prime.

19. $2.(p-3)! \equiv p-1 \pmod{p^2-p}$ if p is prime and greater than 3.

20. $4.(p-3)! + p \equiv -2 \pmod{p^2-2p}$ if p and $p-2$ are prime.

21. $(2p-1)! - p \equiv 0 \pmod{p^2}$ if p is prime.

22. If $4q+3 = p$ where p is prime, prove that

(i) $(2q+1)! \equiv \pm 1 \pmod{p}$ (ii) $(2q)! \equiv \pm 2 \pmod{p}$.

23. If q is odd, prove that

$$(2q-1)! \equiv q!\,(q-1)! \pmod{q^2 q!}.$$

24. Prove that an integer of the form $9n \pm 4$ cannot be expressed as the sum of three cubes.

C

25. If $a_1, a_2, \ldots$ are integers and if p is prime, prove that $(\Sigma a_r)^p = \Sigma a_r^p \pmod p$ and deduce Fermat's theorem.

26. Prove that $n^{12} = 1 \pmod{65520}$ if n is prime to 2730.

27. Prove that $18! = -1 \pmod{437}$.

28. Prove that $3.5.7 \ldots (p-2) = \pm 1 \pmod p$ if and only if p is prime and $p = 3 \pmod 4$.

29. Use the squares of 23 and 24 to show that 31 is a residue and 5 is a non-residue (mod 83). Solve (i) $5^x = 1 \pmod{166}$, (ii) $31^y = 1 \pmod{166}$.

30. If $2q+1$ is an odd prime and a is prime to it, prove that $a^2, (2a)^2, (3a)^2, \ldots, (qa)^2$ are all incongruent (mod $2q+1$).

31. Prove that if each of two integers is the sum of two squares, so also is their product.

Given $533 = 23^2 + 2^2 = 7^2 + 22^2$, $1037 = 29^2 + 14^2 = 19^2 + 26^2$, show how 533×1037 can be expressed as the sum of two squares in eight ways.

32. Prove that an integer of the form $16n - 1$ cannot be expressed as the sum of fewer than 15 fourth powers.

33. Show that the number of regular polygons of n sides which can be inscribed in a given circle having one vertex given is $\frac{1}{2}\phi(n)$.

34. Show how the 59 hexagons having the same vertices as a given regular hexagon can be arranged in :

(i) 7 sets of 6 congruent hexagons

(ii) 5 sets of 3 congruent hexagons

(iii) 1 set of 2 congruent hexagons.

35. Factorise

$$(ax - by + cz - dt)^2 + (ay + bx + ct + dz)^2 + (cx + dy - az - bt)^2 + (at - bz - cy + dx)^2.$$

It follows that the product of two integers each the sum of four squares can also be expressed as the sum of four squares.

36. Solve in integers $x^2 + y^2 = 2z^2$ by reducing it to the form $a^2 + b^2 = c^2$.

MISCELLANEOUS EXAMPLES

EXERCISE XIXe

A

Prove the congruences in Nos. 1-4.

1. $11.3^n + 3.7^n = 6 \pmod 8$.

2. $2^{3n+2} + 21n = 4 \pmod{49}$.

3. $(n^2-1)^2(n^2-4) = 0 \pmod{8640}$ if n is prime to 30.

4. $(q-2).(q-1)! = 2 \pmod{q^2+2q}$ if q, $q+2$ are prime.

5. Solve $5x = 6 \pmod 7$.

6. Solve $2x^2 + 6x + 3 = 0 \pmod{13}$.

7. Find the number of integers less than $(n^2+1)^r$ which are divisible by n but not by n^2.

8. Prove that $\sum_{r=1}^{p} \{a + (r-1)d\}^{p-1} = -1 \pmod p$ if p is prime and d is prime to p.

9. Prove that $(mn)!$ is divisible by $m!(n!)^m$.

10. If x, y are co-prime, prove that $x^2 + 3y^2$ is not divisible by 17.

11. Prove that there is an unlimited number of primes of the form $4n-1$.

12. Prove that (i) $2^{23} = 1 \pmod{47}$, (ii) $2^{43} = 1 \pmod{431}$. [This is a verification of Mersenne's property for $n = 23, 43$.]

B

Prove the congruences in Nos. 13-15.

13. $n^5 - 5n^3 + 4n = 0 \pmod{120}$.

14. $p^2 = 1 \pmod{24}$ if p is prime and greater than 3.

15. $3^{2n+3} + 40n = 27 \pmod{64}$.

16. Solve $31x = -1 \pmod{71}$. 17. Solve $5x^2 = 3 \pmod{17}$.

18. Verify that 16×1151 and $16 \times 23 \times 47$ are amicable (see Exercise XIXa, No. 4).

19. Prove that $2^{32} = -1 \pmod{641}$.

20. If x and y are co-prime, prove that $x^4 + 3y^2$ is not divisible by 5 or by 11.

21. Prove that $\sum_{r=1}^{p} \{(r-1)!\,(p-r)!\} \equiv -1 \pmod{p}$ if p is an odd prime.

22. Factorise $2^{4n+2}+1$ by using the quadratic factors of $4x^4+y^4$.

23. If a is divided by b, the quotient is q and the remainder r. Prove that if a and bq are divided by r, the remainders are equal and the quotients differ by unity.

24. Show that the product of two sums of three squares can be expressed as the sum of four squares, by factorising

$$(ax+by+cz)^2+(bz-cy)^2+(cx-az)^2+(ay-bx)^2.$$

25. Express n^3 as the sum of n consecutive odd numbers.

C

26. Prove that $3^p-2^p \equiv 1 \pmod{49p}$ if p is a prime of the form $6n+1$.

27. Solve $x\{(p-4)!\} \equiv 1 \pmod{p}$ if p is prime.

28. Prove that 2^n-1 is not prime if n is not prime.

29. Prove that $2^n \equiv 2 \pmod{n}$, if $n = 37 \times 73$.

30. If α, β are any two of 1, 2, ..., $p-1$, where p is prime, prove that $\sum(\alpha\beta)^{p-1} \equiv 1 \pmod{p}$.

31. If P is the product of all positive integers less than n and prime to it, prove that $P^2 \equiv 1 \pmod{n}$.

32. If $s_r = 1^r+2^r+\ldots+(p-1)^r$, where p is prime, prove that $s_1, s_2, \ldots, s_{p-2}$ and $s_{p-1}+1$ are all divisible by p.

33. Prove that $2^n! \equiv 0 \pmod{2^n 2^{n-1}!\,2^{n-2}! \ldots 8!\,4!\,2!}$.

34. Use the quadratic factors of x^6+3y^6 to express $3^{6n+3}+1$ as the product of three integers.

35. Prove that the product of n consecutive odd numbers is a multiple of the greatest odd factor of $n!$

36. If a, m, n are positive integers of which m, n are co-prime, prove that $1+a+a^2+\ldots+a^{m-1}$, $1+a+a^2+\ldots+a^{n-1}$ are co-prime.

37. Prove that every factor of n^4+3n^2+1 is of the form $4r+1$.

38. If p is prime, prove that the sum of the products $p-2$ at a time of 1, 2, 3, ..., $p-1$ is divisible by p^2.

39. If the lengths of the sides of a right-angled triangle are all measured by integers, prove that the area is not measured by a perfect square.

ANSWERS

Page 371 EXERCISE XVa

1. $1<x<\frac{3}{2}$ or $2<x$ 2. $-\frac{1}{2}<x<\frac{3}{4}$ 3. All x.

4. $x<\alpha$ or $0<x<\beta$ 5. $(a<0, b^2<ac)$ or $(c<0=a=b)$.

12. $\frac{1}{3}k^2$ 13. $x>2$ 14. $2<x<3$ 15. $|x|>5$

16. $x<-2$ or $x>5$ 17. $x<\frac{1}{2}$ 18. $\frac{1}{2}\sqrt{15}<|x|<\frac{1}{2}\sqrt{7}$

19. No x 20. $x<-1$

21. (i) $x+y>0$, $x\neq y$; (ii) $|x|$, $|y|$ separated by 1.

22. (i) $a+b\geqslant 2\sqrt{ab}$, (ii) $\sum a^2\geqslant\sum ab$,
(iii) $(n-1)\sum a_r^2\geqslant\sum\sum a_r a_s$; a, b, $\therefore$ not all equal.

24. $2\sqrt{cd}$ 37. $[a]$, $[b]$, $[\sqrt{c}]$ not all proportional

Page 378 EXERCISE XVb

1. $\frac{1}{4}c^4$ 2. $\sqrt{(3^5 5^5 8^{-4})}$ 11. 1.

12. $4c^{-4}$ 13. $7^5/(2.5^7)$ 24. $9c^3$

Page 382 EXERCISE XVc

2. $b_\mu=a_\mu\{np_\mu/\sum p\}^{1/r}$ 10. (i) $\leqslant$, (ii) $\geqslant$. 22. $<$ becomes $>$.

Page 388 EXERCISE XVd

4. $y^{\alpha/\beta}$

22. $\frac{1}{2}r(1-r)(1-x)^2<1-x^r-r(1-x)<\frac{1}{2}r(1-r)(1-x)^2x^{-2}$.

Page 390 EXERCISE XVe

4. $k^m n^{1-m}$ 11. $-2<x<0$ or $2<x<3$.

Page 396 EXERCISE XVIa

1. -1 2. -1 3. $+1$ 4. $+1$ (a, b, c, d unequal)

5. 0 6. 0 7. $x_1^2+x_2^2$ 8. $a_1b_1+a_2b_2+a_3b_3$

9. $x_{\alpha 1}y_{1\beta}+x_{\alpha 2}y_{2\beta}+x_{\alpha 3}y_{3\beta}$ 10. $a_{1p}^2+a_{2p}^2+a_{3p}^2+\ldots$

11. $\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}$ 12. $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$ 13. $\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}$

14. $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$ 16. (i) Any line; (ii) a conic circumscribing triangle of reference; (iii) a line-pair.

17. 6. 18. -1 19. -1 20. 2

21. (i) 1, 3, 4 or 1, 4, 6; (ii) 1, 2, 4 or 1, 4, 5; (iii) 2, 3, 6 or 3, 5, 6.

23. $\sum a_n y_n z_n = 0$ (both parts) 24. $(-1)^{n-1}$ 25. $(-1)^{n(n-1)/2}$

26. $(-1)^{n(n-1)/2}$ 27. 6 28. 6 $\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}$

30. A conic and the polar of $(y_1y_2y_3)$.

Page 402 EXERCISE XVIb

1. $+$ 2. $-$ 3. $-$ 4. $+$ 5. 0

6. $(b-c)(c-a)(a-b)$. 8. $-\frac{1}{2}(a+b+c)$

9. $(b-c)(c-a)(a-b)\sum(a^2+bc)$

10. $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)(a+b+c+d)$

11. $a(b-a)(b-c)(c-d)$ 12. $-$ 13. $+$ 14. $-$

16. 0. 17. a^4 18. a, b, c

19. $3(y-z)(z-x)(x-y)\sum(x+yz)$

23. $a+\mu b+\mu^2 c+\mu^3 d+\mu^4 e$, $\mu = \operatorname{cis}\frac{2}{5}k\pi$, $k = 1$ to 5.

24. $(b-c)(c-a)(a-b)(\sum a^3+\sum a^2b+abc)$.

Page 412 EXERCISE XVIc

1. $-\ -\ -$

2. $-(a_{23}a_{44}a_{55})$; $-(a_{14}a_{35}a_{66})$; $+(a_{14}a_{25}a_{36}a_{77})$

3. $\sum(a^4-2b^2c^2)$ 4. 0 6. a^2, $(af-be+cd)^2$.

7. Rows: $c^2, -cb, ca$; $-bc, b^2, -ba$; $ac, -ab, a^2$

10. $abc + 2fgh - af^2 - bg^2 - ch^2 = 0$. 12.

13. $+(a_{11}a_{42}a_{34})$ 14. $\sum(a^4 - 2b^2c^2)$

15. $\sum\{a(y_1z_2 - y_2z_1)^2 + 2f(z_1x_2 - z_2x_1)(x_1y_2 - x_2y_1)\}$

16. $(ap + bq + cr + ds)^2 + (-aq + bp - cs + dr)^2$
$+ (-ar + bs + cp - dq)^2 + (-as - br + cq + dp)^2$

18. $4a^2b^2c^2$ 23. Rows: a, b, c; c, a, b; b, c, a.

25. Rows: $\alpha^2, \alpha^2, \alpha, 1, 0$; $\beta^2, \beta^2, \beta, 1, 0$; $\gamma^2, \gamma^2, \gamma, 1, 0$;
$0, 0, 0, 0, 1$; $y^2, y^2, y, 1, 0$.
$-(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2(x-\alpha)(x-\beta)(x-\gamma)(y-\alpha)(y-\beta)\times$
$(y-\gamma)$.

26. $0 = 0$.

Page 416 **EXERCISE XVId**

1. $\Pi(cy - bz)$ 2. $\Pi(1 + \lambda a + a^3)$, $\lambda = \pm 1, \pm\sqrt{3}$

5. $\pm(x^3 + y^3 + z^3 - 3xyz)$ 7. $\sum a^p b^q c^r d^s$, $p + q + r + s = n$.

10. 0. 11. $(\sum a^2)^3$

12. p^{th} column: $a_{1\mu}b_{\mu p}$, $a_{2\mu}b_{\mu p}$, b_{3p}, b_{4p}

14. $2de^2(a^2 - c^2)$ 17. $(x^2 + a^2 + b^2 + c^2)^3$.

18. $(-1)^n(x^n - u_0x^{n-1} + u_0u_1x^{n-2} - \ldots$ to $n+1$ terms).

Page 430 **EXERCISE XVIIa**

1. 1, 2, 3, 4 2. They coincide 3. 1, 1, 2

5. Yes, yes.

7. $-4 : 5 : 1$; $x = 0, y : z = 1 : -3$; $y = 0, x : z = 1 : -4$

8. 3, 1, 2; $\delta = \epsilon = 3$ 9. No solution; $\delta = 2, \epsilon = 3$

10. $7 - 2k, k - 1, k$; $\delta = \epsilon = 2$ 11. $3 : 1 : 2 : 1$

12. $x : y : z = -2 : 1 : 1, t = 0$ 14. $a + 2b = 7c$

15. No solution; $\delta = 2, \epsilon = 3$ 16. No solution; $\delta = 1, \epsilon = 2$.

17. $3 - k, k, 2 - k$ 18. $6k + 3, 5 - k, 1 - 5k$

19. $a_1(a_3 - a_1)(a_2 - a_1)x_1 = b(a_3 - b)(a_2 - b)$, etc.

20. $a = -2$, no solution; $a = 1$, $x = k$, $y = k'$, $z = 1 - k - k'$;
otherwise, $-(a+1)/(a+2)$, $1/(a+2)$, $(a+1)^2/(a+2)$

Page 437 EXERCISE XVIIb

[α means 'add corresponding elements', β means 'repeat the previous answer', γ means 'does not exist']

1. α, $\begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$, $\begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$ 2. α, γ, γ

3. α, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} ab & b^2 \\ -a^2 & -ab \end{bmatrix}$

4. γ, $\begin{bmatrix} 1 & 3 & 5 & 7 \\ 3 & 7 & 11 & 15 \\ 5 & 11 & 17 & 23 \\ 7 & 15 & 23 & 31 \end{bmatrix}$, $\begin{bmatrix} 6 & 10 \\ 34 & 50 \end{bmatrix}$

5. (i) $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, β; (ii) $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$, $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix}$

6. 3, 8 7. $[\sum(ax^2+2fyz)]$

9. $A^2+AB+BA+B^2$; A and B conformable and square.

10. O. 11. α, O, β

12. α, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

13. α, $\begin{bmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{bmatrix}$, β 14. γ, γ, O

16. B, C conformable. Number of cols of A = number of rows of B

17. $A^2-AB+BA-B^2$; A, B conformable and square

18. $-k$, i

19. $\begin{bmatrix} a-\delta b & -c-\delta d \\ c-\delta d & a+\delta b \end{bmatrix}$ 20. $\begin{bmatrix} 2 & 2 & 2 \\ 4 & 4 & 4 \end{bmatrix}$, $\begin{bmatrix} 11 & 2 \\ 14 & 2 \end{bmatrix}$

Page 450 EXERCISE XVIIc

1. $\begin{bmatrix} a_{11}+k & a_{12} & a_{13} \\ a_{21} & a_{22}+k & a_{23} \\ a_{31} & a_{32} & a_{33}+k \end{bmatrix}$

2. $\begin{bmatrix} 10 & -5 \\ -8 & 3 \end{bmatrix}$, $\begin{bmatrix} -1 & \cdot 5 \\ \cdot 8 & -\cdot 3 \end{bmatrix}$, $\begin{bmatrix} -2 & +6 & -4 \\ -1 & -6 & +5 \\ +2 & +2 & -2 \end{bmatrix}$, $\begin{bmatrix} -1 & +3 & -2 \\ -\cdot 5 & -3 & 2\cdot 5 \\ +1 & +1 & -1 \end{bmatrix}$; determinants of the transposed matrices

4. $y_\nu = A_{\mu\nu} x_\mu \div |a_{\mu\nu}|$ 5. $\begin{bmatrix} 9 & 15 \\ 12 & 27 \end{bmatrix}$, $\begin{bmatrix} 38 & -1 \\ 139 & -2 \end{bmatrix}$

6. No solution.

12. $\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$ 14. $\begin{bmatrix} -12 & -12 & 9 \\ -6 & -13 & -4 \\ +3 & -6 & -18 \end{bmatrix}$

18. 34 19. $x : y = 3 : -2,\ z = t = 0$

20. No meaning if $ab = 0$. No solution if $a = b$ unless $a = 1$ when $x = k$, $y = k'$, $z = 1 - k - k'$. Otherwise,

$$a^2(1-b)/(a-b),\ b(a^2-1)/(a^2-ab),\ (1-a)/(a^2-ab).$$

22. $x_\mu = b_\nu a_{\nu\mu} \div |a_{\mu\nu}|$

26. $a_{\lambda\mu} b_{\mu\lambda}$, $a_{\lambda\mu} b_{\mu\nu} c_{\nu\lambda}$, yes, no. 27. $(-1)^{rs+tu} : 1$

29. $A_{\mu\nu} A_{\mu q} = A_{\nu\nu} A_{q\nu} = |a|^2 \delta^q_p$ (1 to n).

Page 459 EXERCISE XVIIIa

1. $3 \cdot (3n-1)! \div \{6^n \cdot (n-1)!\}$ 2. 7^{26} 3. 75600

4. $n!\,(n-1)! \div \{(n-r)!\,(r-1)!\}$

5. $(2n-1)! \div \{n!\,(n-1)!\}$ 6. $\frac{1}{3}(n+1)(2n^2+4n+3)$

7. $\frac{1}{2}(n+1)(n+2)$, $\frac{1}{2}(b+1)(2n-b+2)$

8. 3003 9. 519156 10. 2, 9, 265

13. 1001 14. 3276

15. $14702688 \equiv 18!/(7!\,6!\,5!)$ 16. 6720

17. $n!\,(n-1)!$ 18. 15 19. $\frac{1}{8}(n-3)(n^2-9n+26)$

20. 10 21. 25 23. $2^{n-1}(n+2)$

24. 1820, 330 25. $r(3n-r) - \frac{3}{2}n(n-1) + 1$

26. (i) $n!\,(n-1)!\div\{(r-1)!\,(n-r)!\,r!\}$;
(ii) $n!\,\Sigma(n-1)!\div\{(r-k)!\,(n-r-1+k)!\,(r-k+1)!\}$
for $k=1$ to r

27. (i) $n!\,(n-1)!\div\{(r-1)!\,(n-r)!\}$; (ii) $(n+r-1)!\div(r-1)!$

30. $\frac{1}{6}n(n^2+6n+11)$ **31.** $n(n^2-1)$

33. $\frac{1}{24}n(27n+1)\,.\,(n+2)!$

35. $\frac{1}{8}\sqrt{5}\{(1+\sqrt{5})^{n+1}-(1-\sqrt{5})^{n+1}\}2^{-n-1}$

Page 474 EXERCISE XVIIIb

1. $\frac{1}{312}$, $\frac{1}{4}$ **2.** $\frac{19}{144}$ **3.** $p_1p_2(1-p_3)$, $p_2(1-p_1)(1-p_3)$

4. $\frac{631857}{1631364}$ **5.** $\frac{3}{4}$ **7.** $\frac{1822258}{1056853}$ **8.** 31s

10. $b-(b-c)/(b+c)$ **11.** $\frac{17}{30}$ **12.** £3 11s 6d

13. £3 8s 4d **14.** $\frac{1}{8}$ **15.** $\frac{63}{256}$, $\frac{319}{512}$

16. $\frac{261}{3888}$ **17.** $6(n-3)\div(n-1)(n-2)$

18. $1-\frac{1}{4}(p+q)$; (i) $m=n$ or $p=q$;
(ii) $(m>n, p>q)$ or $(m<n, p<q)$

20. $\frac{1}{4}$ **21.** £2 5s 9d **22.** $1{\cdot}6\times10^{-18}$

24. $\frac{1}{2}\sqrt{3}$, $\frac{3}{5}$, $\frac{1}{2}$ **25.** 137 **26.** $\frac{9}{25}$

Page 477 EXERCISE XVIIIc

1. $2^{n-p}(p+1)-1$ **2.** 105 **3.** 4096, 1560

4. $\frac{5}{18}$ **5.** $\frac{17}{27}$ **6.** $\Sigma pqr-4\Sigma pqrs+10pqrst$

7. $\frac{4}{385385}$ **8.** $1-(\frac{31}{36})^n$ **9.** $\frac{1}{2}$

10. $\frac{1}{3}\{2+(-2)^{-n}\}$ **11.** $\frac{91}{256}$ **13.** 4^{14}

14. $(p+1)(q+1)(r+1)-1$ **15.** $\frac{1}{2}n(n+1)$

16. $\frac{1}{6}\{(n+1)(n+2)(n+3)-(n-a)(n-a+1)(n-a+2)\}$

17. 4 **19.** 2943360 **21.** $\frac{5}{12}$

22. $\Sigma(-1)^{k-1}\binom{r}{k}\left(1-\frac{k}{n}\right)^n$ for $k=1$ to r.

25. $\frac{1}{2}-\frac{1}{2}\{(y-x)/(y+x)\}^n$ **28.** $(n-1)/(4n+2)$

30. $a/(a+b)$ **31.** ·001 **33.** $1-52!/52!$, $\doteq$·632

34. $u_n=(1-u_1-\ldots-u_{n-3})\times\frac{2}{3}\times\frac{1}{3}$
$=\{(\sqrt{5}+1)^{2n-1}+(\sqrt{5}-1)^{2n-1}\}/(12^n\sqrt{5})$.

Page 484 EXERCISE XIXa

1. 22 2. 12, 14 5. 36 6. 720
8. $\frac{1}{2}m+r$ where $m=(n+1)!$ and $r=2$ to $n+1$
9. 1·26, ·92; 1·19, ·87 11. 4 14. 16
16. 1·07, ·9995 17. 10078
18. $2^n(p+2)-p-1$, $2^n(pq+2p+2q+2)-(p+1)(q+1)$
26. $6/\pi^2$ (·61)

Page 491 EXERCISE XIXb

2. x not integral 3. 164 4. 2400 13. 249
21. 48000 24. 6

Page 499 EXERCISE XIXc

5. 3 6. 4 7. 3 8. 55
9. 3 10. 3, 8, 13, 18, 23, 28 11. 38(mod 77)
12. 7, 10 13. 7, 12 14. No solution 15. 5, 14
16. 11, 44 17. 3, 6 18. 6, 11 19. 2, 6, 7, 8, 10
20. $a=3$, $x=\pm 3$; $a=5$, $x=\pm 1$; $a=6$, $x=\pm 2$
27. 5, 3, 1, 6, 4, 2; 6, 3, 0; 10, 8, 6, 4, 2, 0 28. 4.
29. 3. 30. 2. 31. 2. 32. 2, 5, 8, 11, 14.
33. 113. 34. 5 35. 7, 20, 33
36. 4, 21, 38, ..., 310 37. 31, 41 38. 20, 80
39. 7, 8 40. 1, 3, 4, 9, 10, 12 42. 1.
43. 36. 44. 162.
47. $(ba)-(dc)+\ldots=0$; same as for 9, 11 in the scale of 10
48. ± 2 (mod 5), ± 2 (mod 7); ± 2 (mod 35), ± 12 (mod 35); $x^2=4$ (mod 35)
50. ± 10 (mod 49) 52. ± 1; $\pm 1, \pm 3$; $\pm 1, \pm(2^{k-1}-1)$.

Page 506 EXERCISE XIXd

29. 82; 41, 82

34. If *ABCDEF* is regular, the sets are like (i) *ABCDFE*, *ABFCDE*, *ABCFDE*, *ADCFBE*, *ACDFBE*, *ABFDCE*, *ACBEDF*, (ii) *ABFDEC*, *AFCDEB*, *ACFDBE*, *ABFCED*, *ADCEBF*, (iii) *ABEFCD*.

35. $(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)$

36. $k(a^2+2ab-b^2)$, $k(a^2-2ab-b^2)$, $k(a^2+b^2)$

Page 509 EXERCISE XIXe

5. 4. 6. 3, 7. 7. $(n-1)\{(n^2+1)^r-1\}/n^2$

16. 16 17. 2, 15.

22. $(2^{2n+1}+2^{n+1}+1)(2^{2n+1}-2^{n+1}+1)$

24. $(a^2+b^2+c^2)(x^2+y^2+z^2)$

25. $\sum(n^2-n+2r-1)$ for $r=1$ to n 27. 6.

34. $(3^{2n+1}+1)(3^{2n+1}+3^{n+1}+1)(3^{2n+1}-3^{n+1}+1)$.

INDEX

Volume I, pages 1-194
„ II, „ 195-366
„ III, „ 367-510

INDEX TO VOLUMES I, II AND III

LIST OF SPECIAL SUMS LIMITS SERIES AND SYMBOLS